Driving innovation together

DPIA on Nextcloud Enterprise

SURF Vendor Compliance

Authors: Sjoera Nas (Privacy Company), Julian Rill and Shiyona Keenakkottil (SURF)
Version: 1.0
Date: 16 July 2026

Revision History

Version	Date	Author(s)	Changes
0.1	18-02-2026	Sjoera Nas (Privacy Company), Julian Rill and Shiyona Keenakkottil (SURF)	Draft DPIA – Part A
0.2	17-04-2026	Sjoera Nas	Part A track changes after input Nextcloud two April 2026 and dialogue 14 April 2026
0.3	17-05-2026	Sjoera Nas	added Part B and D after input Nextcloud 6 May and dialogue 8 May 2026
0.4	28-05-2026	Sjoera Nas	added part C and Summary, processed input SURF, flagged missing information for Nextcloud with yellow highlights.
0.5	02-07-2026	Sjoera Nas	Track changes after agreement on DPA
0.6	02-07-2026	Sjoera Nas and Sophia Gelpke (SURF)	Clean version for company confidentiality review by Nextcloud
0.7	06 and 07-07-2026	Sophia Gelpke	Track changes Nextcloud input
0.8	13-07-2026	Sjoera Nas	Final draft version track changes
0.9	13-07-2026	Sjoera Nas	Final prepublication version clean
1.0	16-07-2026	Sjoera Nas	Final publication version clean

Review Record

Version	Date	Reviewer(s)	Notes
0.1	2 April 2026	Nextcloud	
0.2	6 May 2026	Nextcloud	
0.3	6 and 7 July 2026	Nextcloud	Company confidentiality input

Table of Contents

List of Figures and Tables

Glossary

Abbreviation	Term
DPA	Data Processing Agreement (amended version to be negotiated by SURF with Nextcloud)
Dutch DPA	Dutch Data Protection Authority (Autoriteit Persoonsgegevens)
DPIA	Data Protection Impact Assessment
DTIA	Data Transfer Impact Assessment
EDPB	European Data Protection Board
Education organisations	Dutch research and education organisations
Nextcloud	Generally used in this report for the company Nextcloud GmbH. When this report mentions the software, it says 'the Nextcloud software'. Sometimes GmbH is added to avoid possible confusion with the software.
SURF	The Dutch collaborative organisation for IT in Dutch higher education and research
SVC	SURF Vendor Compliance

Summary

This document is a DPIA (Data Protection Impact Assessment) on the Nextcloud Enterprise Office software. The DPIA is commissioned by SURF, the collaborative organisation for IT in Dutch higher education and research, sometimes abbreviated to 'The Dutch education sector' or 'education organisations'. The report is written by Privacy Company in coproduction with SURF.

Nextcloud software
Nextcloud Enterprise is an open-source software suite. Organisations that wish to use this software have to host the software themselves, or look for a third party hosting provider. The software is developed/maintained by the German company Nextcloud GmbH, with the help of external software developers. Nextcloud itself does not offer Nextcloud Enterprise as a cloud service, though it links to Nextcloud Partners that can offer the software as fully managed SaaS.

Scope of the DPIA
The scope of this DPIA is limited to Nextcloud Files (filesharing), Groupware (email, calendar, contacts and deck), Talk (videoconferencing and chat) and Nextcloud Office (tested with Collabora Online). Additionally, SURF tested the generative AI transcription facility for video calls in Talk. End users can access the different Nextcloud software bundles via a web interface. SURF also tested with Files and Talk installed on Windows and on MacOS. This DPIA includes a security assessment (Chapter 6).

Outcome: 15 low data protection risks
The outcome of this DPIA is that there are 15 low data protection risks. The risks and mitigating measures are shown in more detail in the table at the end of this summary. Additionally, this DPIA contains a provisional list of essential security measures organisations must take to prevent data protection risks when they decide to host the software themselves (Section C.1.1.1).

Personal data
This DPIA is based on a legal analysis of the available public documentation about the tested Nextcloud software, the replies from Nextcloud to questions from SURF, the contents of the negotiated amended Data Processing Agreement, the findings in the Technical Appendix and part A of the DPIA as well as a technical examination of the outgoing network data.

To better understand the data processing, both inside of the software and in data shared with Nextcloud, SURF hosted the software itself, created 2 end users and 1 administrator (after this: admin), and performed a number of scripted scenarios with the 3 users. SURF also accessed the available logs in the software, and filed a Data Subject Access request with Nextcloud.

This report distinguishes between 5 categories of personal data processed inside of the software, or processed by Nextcloud GmbH:

1. Content Data (only available to customers, inside the self-hosted Nextcloud software)
2. Account Data, in two types:
   a. Admin Account Data
   b. Contact Data from procurement officers
3. Diagnostic Data, in three types:
   a. Logs only available to customers
   b. Logs optionally shared by customers with Nextcloud
   c. Logs created by Nextcloud GmbH
4. Support Data (both the contents of support tickets and metadata)
5. Website Data, in two types:
   a. the restricted access websites, i.e. the admin and support portal, and
   b. the publicly available nextcloud.com pages with relevant technical documentation, the form to request data subject access, and legal information.

A key difference with cloud providers of productivity software is that the company Nextcloud collects very little personal data. Nextcloud for example has not programmed the software applications to automatically send Telemetry Data to the company and cannot access any data processed in the customer environment, not even for support purposes.

Purposes, roles and legal grounds
Initially, Nextcloud took the position that it only was a data processor for the content of support tickets. The technical analysis showed that Nextcloud processed more categories of personal data. As a result of the negotiations with SURF, Nextcloud has agreed to also become a data processor for the limited personal data it collects: admin Account, Diagnostic and restricted access Website Data. Nextcloud can process these personal data for 4 specific purposes, namely:

1. Technically provide the Software and applications via portal.nextcloud.com (Process visitor and download information);
2. Provide third level support/technical assistance based on third line requests from Customers;
3. Help secure Personal Data Processed by the Customer in the Software by sending update notifications and newsletters about technical updates and security developments to admins;
4. Technically improve the Software and Services for all Customers, including bug fixing, troubleshooting, patching, and general maintenance by using the aggregated Support and voluntarily provided Diagnostic Data.

Since every supplier needs to use some personal data from its customers for its own legitimate business purposes, for example, to send invoices, SURF and Nextcloud have also agreed on a limitative list of seven specific authorised *further processing* purposes. This means Nextcloud can process these data as controller, when strictly necessary and proportionate for these purposes, and within the conditions agreed in the amended Data Processing Agreement. In abbreviated form these seven purposes are:

1. Comply with legal obligations
2. Billing, fulfilling of orders and receiving payments

3. Customer relationship management
4. Licensing compliance/fraud detection
5. Use statistical data for internal reporting, financial reporting, prioritising security patches, and product strategy
6. Create statistical website analytics from the restricted access websites.
7. Use statistical data to technically improve and optimise the performance and efficiency of the software

This DPIA assesses that further processing for these purposes is *compatible* with the purposes for which Dutch education organisations enable Nextcloud as a processor to collect personal data, in line with the requirements of Article 6(4) of the GDPR.

International data transfers
Nextcloud aims to be the only serious European alternative for Microsoft and Google and stresses data sovereignty as a key reason to adopt its products. Nextcloud contractually assures it will reject requests for disclosure from non-EU government authorities, and will take the agreed steps to prevent or at least minimise disclosure to EU authorities. Nextcloud has also provided extensive assurances that it has not, and will not, build backdoors in the software that may lead to access for government authorities. The security of the software was recently audited by the German cyber security authority BSI, and Nextcloud was awarded a CSPN certificate.

However, Nextcloud uses an outbound mail delivery provider from the USA. During testing, the admin was automatically subscribed to both a security and a commercial newsletter from Nextcloud, and the admin and Nextcloud communicated about this DPIA. This US supplier keeps logs with the contents of the emails plus detailed technical information about the recipient. Nextcloud will switch to a native EU-provider in Q3 2026.

SURF used Nextcloud's Office software built on Collabora Online from the UK company Collabora. This means Collabora employees in the UK can access the relevant support tickets in Nextcloud's central support ticketing system. Nextcloud has committed to only provide access to EU-based employees if the adequacy decision for the UK becomes invalid.

Additionally, Nextcloud relies on two US American software repositories for essential security updates and information, GitHub and Hugging Face (to download an LLM for Nextcloud Assistant). This DPIA recommends measures for admins to prevent tracking by these platforms.

Data retention and exercise of data subject rights
Nextcloud provided a swift and detailed answer to SURF's Data Subject Access Requests (DSARs). However, 4 categories of personal data were missing. Nextcloud has provided the missing personal data during the DPIA process and committed to provide a full reply to future DSARs.

Nextcloud and SURF have agreed on a retention period of 15 months for support tickets after closure of the case. Admins can ask Nextcloud for earlier deletion of tickets and attachments.

It follows from the technical analysis that Nextcloud GmbH and its subprocessors can process seven types of logs. Nextcloud has explained the retention periods to SURF, and has committed to publish the details in July 2026, as approved by SURF. Similarly, Nextcloud has committed to improve the central documentation about the many logs that can be generated inside the software, and their default retention periods (or default maximum storage sizes)

Conclusions
Based on the amended DPA for the Dutch education sector, Nextcloud is a processor for the 4 relevant categories of personal data for the 4 agreed purposes, and authorised controller for some of these personal data for the agreed and compatible seven *further processing* purposes. The amended DPA ensures that the education organisations are in control of the processing via sub-processors, can rely on EU-exclusive data processing (plus processing of support tickets in the UK if they choose Collabora Online), self-determine the necessary retention periods, only accept strictly necessary cookies, and can trust SURF to exercise the right to audit compliance with the agreed data protection clauses and measures.

As shown in the table below, based on measures already taken by Nextcloud, and provided the education organisations apply the recommended measures and Nextcloud takes the agreed measures, there are no more known high data protection risks, and only 15 low or solved risks.

No.	Risks	Recommended measures education organisations	Measures taken or committed by NEXTCLOUD	Residual risks
1.	Loss of control purposes processing of admin Account Data in Account, Diagnostic, Support metadata and Website Data	Sign up for Nextcloud Enterprise via SURF, and when signing up via a reseller or provider of a fully managed solution, ensure applicability of the SURF DPA.	Agreed to limitative list of 4 processor purposes in amended DPA.	solved
			Agreed to limitative list of seven authorised further processing purposes (legitimate business operations) in amended DPA.	
			Agreed to 3 explicit processing prohibitions: no further processing for other purposes, no processing for advertising purposes or serve advertising, not for direct marketing, profiling, research or analytics purposes unless the customer instructs Nextcloud to do so, no CSAM scanning.	
		(SURF): use the audit right to verify compliance with purpose limitation, data	Agreed to extensive audit right for SURF on behalf of the education organisations in amended DPA.	

		minimisation and retention periods.	Committed to renew the security code audit for CSPN every 3 years and share the full findings with SURF.	
2.	Loss of control transfer of email addresses to the USA	-	Committed to switch to an EU-based mail delivery provider in Q3 2026.	low
		Instruct admins to prevent sharing their private IP addresses and personal device details when accessing GitHub and Hugging Face.	Nextcloud as a processor only processes data in the EU as agreed in amended DPA, with the exception of subprocessors outside of the EU chosen by customers such as Collabora.	
		Instruct admins to not remain permanently logged-in to GitHub and Hugging Face.	Nextcloud will offer two types of subscription to Enterprise customers in Q3 2026: as commercial contact for a customer or as admin.	
3.	Loss of control transfer Support Data Collabora outside of the EU	-	Limited the access to the relevant Collabora tickets in Zammad to employees physically located in the UK and in the EU.	solved
			Committed to prevent access from employees located in the UK if the adequacy status becomes invalid.	
4.	Loss of confidentiality through security breach	-	Nextcloud will enforce 2FA on the admin and support portal in the new version v7.1 of Zammad's support portal which has been released 1 July 2026.	solved
5.	Loss of control through lack of transparency Diagnostic Data optionally shared by admins	Optional: consider use of pseudonymised admin employee accounts, for example using identity federation to share Usage Survey Data with Nextcloud	Agreed to include Diagnostic Data in expanded scope of the amended DPA.	low
			Retention periods of 3 types of logs optionally shared by admins agreed in amended DPA,	
			Will publicly document these retention periods in July 2026.	
		(SURF): conduct audits on compliance with purpose limitation, data minimisation and retention periods both	Agreed to extensive audit possibilities for SURF in amended DPA.	

		as processor and as authorised controller.		
6.	Loss of control through lack of transparency and risk of reidentification other Diagnostic Data, support metadata, and Website Data	Inform admins about the functional cookies with this umbrella DPIA and instruct them not to change the default settings on the public nextcloud.com website.	Will update information about functional cookies on admin and support portal in July 2026	low
		Inform admins about the existence of the seven identified relevant logs generated by Nextcloud GmbH and its sub-processors and the retention periods.	Nextcloud has provided SURF with additional information about the seven logs. Nextcloud will publish this information on its public website in July 2026 (as approved by SURF).	
		Inform admins about the contents of the Zammad support ticketing system's activity log and retention period of 42 days.	Nextcloud will publish this information on its public website in July 2026 (as reviewed by SURF).	
7.	Loss of control and lack of transparency sub-processors	-	Agreed to procedure to deal with changes in amended DPA, both with regard to new subprocessors and to other changes.	solved
8.	Inability to exercise data subject access rights	-	Committed to provide full access to a DSAR. This includes access to any collected Usage Survey Data, activity logs from the support ticketing system, frozen webserver access logs (provided Nextcloud can reliably verify the identity of the data subject) and logs kept by Postmark (or future EU based mail service provider). *NOTE: SURF has not retested this with a new DSAR.*	low
9.	Inability to exercise data subject rights	Instruct admins to only share strictly necessary personal data in support tickets. Do not	Nextcloud will generally honour requests to delete one or more support tickets and/or attachments, unless there is a legal	low

	to delete Support Data	use support tickets to file legal or financial claims.	reason to retain a specific ticket.	
			Nextcloud has agreed on a maximum retention period of 15 months for closed support tickets for SURF members.	
			In the agreed new public documentation about the logs Nextcloud GmbH collects and retention periods Nextcloud includes it can exceptionally retain the support tickets about a specific topic longer, for a specific legal reason.	
			Nextcloud has already implemented a warning against sharing of personal data in attachments on the admin portal, and will show the warning in the support portal by Q3 2026.	
		Instruct admins to annually ask Nextcloud for deletion of all support tickets after the self determined retention period of for example 13 or 15 months.	Agreed in amended DPA to only process aggregated and pseudonymous data higher than tenant level from support tickets as authorised controller.	
10.	Loss of control disclosure (limited) personal data to public bodies in and outside of the EU		Agreed in amended DPA to proposed risk minimisation steps. Nextcloud will reject requests from non-EU authorities. Nextcloud will try to redirect requests from EU authorities to its customer, legally contest where possible and viable, but if necessary, only disclose the minimum necessary data.	low
			Committed in amended DPA to publish transparency statistics at least once a year, including numbers about received and answered requests.	
11.	Loss of control	Warn admins not to use their Admin	Agreed to two lists of purposes in amended DPA.	solved

	processing Nextcloud independent controller	Account Data to enable processing by Nextcloud or third parties as independent controller, for example by consenting to analytic and tracking cookies. Tell admins to use a pseudonymous account when registering for an event or when registering to download a whitepaper.	Agreed in amended DPA to maintain current privacy by default settings. Analytics and marketing cookies are only placed on the public website after voluntary consent of the user.	
12.	Loss of control: use of tracking pixel in Nextcloud outbound mail	.	Nextcloud has disabled the tracking pixel in its mailings.	solved
13.	Loss of control Admin account data in newsletters	Instruct admins to unsubscribe from commercial newsletters	In the self-service Nextcloud portal (portal.nextcloud.com) customers will be able to register as admin or commercial contact and decide themselves to subscribe and unsubscribe to commercial and technical newsletters in Q3 2026.	low
14.	Loss of control through lack of transparency existence of multiple logs in the software	Use the list in this umbrella DPIA to make admins aware of all available logs.	Nextcloud will provide a better overview of available logs for admins in the existing log documentation in Q3 2026.	low
15.	Chilling effect: employee and student	Make admins aware of the potentially sensitive contents of the (original) audit and Talk interaction logs.	Nextcloud has committed to develop a second export version of the audit and interaction logs, by the end of 2026. Personal data such as meeting and	low

	monitoring system	Update the internal IT policy when these logs can be legitimately used for what purposes.	file names will be masked with ***REMOVED SENSITIVE VALUE***.	
		To prevent use of the audit and interaction logs as employee monitoring system, import the masked version of the Audit and Talk interaction logs in the SIEM and log management tools once available and determine an adequate retention period for the raw data.	Nextcloud will update the available information about the sensitive contents in Q3 2026.	

Introduction

The German company Nextcloud GmbH offers open source software for online work productivity.[1] With Nextcloud Enterprise customers can create and collaborate with text, numbers and presentation files. Nextcloud GmbH itself does not offer the software as a cloud service (SaaS): customers have to install and maintain the software on their own servers, or engage a third party service provider that can offer the software as fully managed SaaS.

The core of Nextcloud's software is Files, as a central source for storage, search and collaboration. The other two core software components developed by Nextcloud itself are Nextcloud Talk (video conferencing and chat) and Nextcloud Groupware (calendar, contacts, mail, deck).

Nextcloud supports several different Office suites, but SURF tested the Office Suite developed by the UK company Collabora. The Nextcloud Office Suite contains multiple web applications to create and collaborate in documents, spreadsheets and presentations. The Nextcloud software is mainly accessed via the web client, but Nextcloud also provides desktop and mobile apps for Talk and Files.

This Data Protection Impact Assessment (DPIA), commissioned by SURF—the Dutch IT cooperative of education and research—describes the personal data processing that occurs on the self-hosted Nextcloud Enterprise servers (data not accessible for the company Nextcloud, only for the admins of the Dutch higher-education and research institutions), and the limited data processing by the company Nextcloud, mainly when the admins ask for support from Nextcloud. This DPIA hence maps two sources of data protection risks for the different categories of data subjects: due to data processing by the customers themselves, and due to the (limited) data processing by the Nextcloud company.

About SURF
SURF is the collaborative organisation for IT in Dutch education and research, owned by its member universities and research institutes. Through SURF, members jointly procure high-quality digital services, develop and share knowledge, and ensure compliance with privacy and security rules. As part of its services, SURF conducts umbrella DPIAs for IT services widely used across the sector.

What is a DPIA?
DPIA stands for Data Protection Impact Assessment. The General Data Protection Regulation (GDPR) requires organisations to perform DPIAs when they process personal data in a way that may '*result in a high risk to the rights and freedoms of natural persons*' (Article 35 GDPR). The assessment should shed light on, among other things, the specific processing activities, the inherent risk to data subjects, and the safeguards applied to mitigate these risks. The purpose of a DPIA is to ensure that all data protection risks resulting from the processing are mapped and assessed, and that adequate safeguards have been implemented or will be implemented to mitigate those risks.

[1] Nextcloud homepage, URL: https://nextcloud.com/ (last visited 19 January 2026).

A DPIA used to be called PIA, *privacy impact assessment*. According to the GDPR a DPIA assesses the risks for the rights and freedoms of individuals. Data subjects have a fundamental right to protection of their personal data and some other fundamental freedoms that can be affected by the processing of personal data, such as freedom of expression. The right to data protection is therefore broader than the right to privacy. Consideration 4 of the GDPR explains:

"This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity".

Umbrella DPIAs versus individual DPIAs
In GDPR terms, SURF is not the data controller for the processing of personal data via the use of
Nextcloud Enterprise. The data controller is the individual educational or research institution that uses this software. However, as the Dutch IT cooperative, SURF takes the responsibility to assess the data protection risks for the end users (including admins) and to ensure the data processing complies with the GDPR. Therefore, SURF conducts umbrella DPIAs to assist its members to select a privacy-compliant deployment.

Nonetheless, this report cannot replace the specific risk assessments the organisations must make themselves. Organisations must still assess their own specific use cases and complement this umbrella DPIA with their own inventory of specific personal data, data subjects, purposes, retention periods and legal grounds. Depending on the chosen technical privacy settings, the nature and volume of the personal data and vulnerability of the data subjects, the processing can lead to other data protection risks.

The performance of an umbrella DPIA has benefits for both SURF's members and for the vendors of the assessed software or service. For the members, it saves time and costs. Through SURF they can share knowledge and experiences with a vendor. Additionally, SURF as representative of the entire sector can more effectively negotiate mitigating measures with vendors. For the vendors, collaborating with an umbrella DPIA saves time, effort and money. First of all, they do not have to assist every institution individually with DPIA questions that will likely be very similar. Secondly, it's more efficient for vendors to get an overview of all relevant measures, and agree on an implementation plan to mitigate all identified risks. Thirdly, vendors can point to the results of the umbrella DPIA as an objective assessment of GDPR-compliance, also to potential new customers.

The Dutch DPA has endorsed this umbrella DPIA approach to improve the protection of personal data within the Education sector.[2]

[2] Dutch DPA (in Dutch only), Sectorbeeld Onderwijs 2021-2023, 24 January 2024, p. 5-6, URL: https://www.autoriteitpersoonsgegevens.nl/documenten/sectorbeeld-onderwijs-2021-2023.

DPIA criteria
The Dutch Data Protection Authority (Dutch DPA) has published a list of 17 types of processing for which a DPIA is always mandatory in the Netherlands.[3] If a processing is not included in this list, an organisation must itself assess whether the data processing is likely to present a high risk. The European national supervisory authorities (hereinafter referred to as the Data Protection Authorities or DPAs), united in the European Data Protection Board (EDPB) have also published a list of 9 criteria.[4] As a rule of thumb, if a data processing meets two of these criteria a DPIA is required.

The circumstances of the data processing via Nextcloud Enterprise meet two out of 17 types of processing from the Dutch DPA's list and 4 out of 9 criteria from the EDPB's list.

Applicable processing types Dutch DPA
The Dutch Data Protection Authority mentions the processing of communications data as specific criterion when a DPIA is mandatory:

"*Communications data (criterion 13). Large-scale processing and/or systematic monitoring of communications data including metadata identifiable to natural persons, unless and as far as this is necessary to protect the integrity and security of the network and the service of the provider involved or the end user's terminal equipment.*"[5]

At the start of this DPIA it was unclear if Nextcloud itself would have access to communications data and metadata in the form of audit logs accessible for the admins in their self-hosted environments, or if the default settings programmed by Nextcloud for the data processing by the education organisations was necessary for the integrity and security of the software.

The Dutch Data Protection Authority also mentions the processing of personal data for employee monitoring purposes as a criterion:

"*Large-scale processing of personal data and/or systematic monitoring of employees' activities*
(e.g. monitoring of email and internet use, GPS systems in employees' cars and lorries, or camera surveillance for the purpose of combating theft and fraud)."[6]

At the start of this DPIA it was unclear how extensive the logs were about the use of the productivity software, if education organisation could use such logs as part of an employee or student monitoring system.

[3] Dutch DPA, list of processings for which a DPIA is required (in Dutch only), Besluit inzake lijst van verwerkingen van persoonsgegevens waarvoor een gegevensbeschermingseffect-beoordeling (DPIA) verplicht is, published in the Staatscourant (Dutch State Gazette) of 27 November 2019, URL: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stcrt-2019-64418.pdf .
[4] EDPB Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01), 13 October 2017, URL: http://ec.europa.eu/newsroom/document.cfm?doc_id=47711
[5] Dutch DPA, list of processings for which a DPIA is required (in Dutch only), 27 November 2019, URL: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stcrt-2019-64418.pdf
[6] Idem.

Applicable EDPB criteria
The circumstances of the data processing via Nextcloud Enterprise (potentially) meet 4 out of the 9 criteria defined by the EDPB:

- Innovative use or applying new technological or organisational solutions (criterion 8). The EDPB explains: "*This is because the use of such technology can involve novel forms of data collection and usage, possibly with a high risk to individuals' rights and freedoms"*[7]
  Even though Nextcloud Enterprise is self-hosted software, it was unclear at the start of this DPIA what data Nextcloud collected about the use of the software, and how the AI-functionality processed personal data ((integrated in the platform, but only tested as part of Talk and not activated automatically).
- Sensitive data or data of a highly personal nature (criterion 4). The EDPB explains: "*some categories of data can be considered as increasing the possible risk to the rights and freedoms of individuals. These personal data are considered as sensitive (as this term is commonly understood) because they are linked to household and private activities (such as electronic communications whose confidentiality should be protected).*"[8]
- While the locally processed Nextcloud logs (only available for customer admins) are neither designed, nor marketed as a tool for behaviour monitoring, there is a possibility that the logs available for admins can be used for systematic observation of the behaviour of employees (criterion 3)[9]; and
- The processing involves data relating to vulnerable data subjects (criterion 7). Students/teachers and admins whose personal data are processed through Nextcloud Enterprise are in an unequal relationship of power with the education organisations. This also includes external people such as future students, job applicants, business relations, and all people that send and receive email to Nextcloud mail users.

Timeline of this DPIA
This data protection impact assessment was carried out by SURF (technical and security research) and Privacy Company (legal assessment) between December 2025 and May 2026.

Outline
This Data Protection Impact Assessment assesses the use of Nextcloud Enterprise by Dutch education organisations, both self-hosted and as future service that may become part of central service offers by SURF.

The Dutch government DPIA-model 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

[7] EDPB Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01).
[8] Idem.
[9] Nextcloud replied that its philosophy is to trust the admin. Nextcloud reply to part A of this DPIA, 2 April 2026.

Part A contains the facts about the data processing via the tested Nextcloud Enterprise software, self-hosted by education organisations or as part of a future central service offered by SURF. This part starts with a description of the functionalities of Nextcloud Enterprise, and the 5 core services tested for this DPIA. This part describes the categories of personal data and data subjects that may be included in the processing; the purposes of the data processing; the different GDPR roles of the involved parties; the different interests related to the tested data processing; the locations where the data are processed, and the retention periods. Part A also lists the relevant legal documents that govern the data processing resulting from the use of Nextcloud Enterprise, addresses the applicability of the ePrivacy Directive and includes a separate section on the relevant technical and organisational security measures.

Part B provides an assessment of the lawfulness of the data processing through Nextcloud Enterprise. This analysis starts with an assessment of the conformity with the key principles of data processing, starting with the legal ground for the processing and the necessity and proportionality of the processing. This part continues with an analysis of compliance with purpose limitation, as well as transparency and data minimisation. In this section the legitimacy of any transfers of personal data to countries outside of the (European Economic Area (EEA) is separately addressed, as well as an analysis how Nextcloud treats requests from data subjects (including admins) to exercise their rights.

Part C assesses the risks to the rights and freedoms of the data subjects caused by the processing activities identified in Part A of this DPIA. It names specific risks resulting from these processing activities and aims to determine both the likelihood that these risks may occur, and the severity of the impact on the rights and freedoms of the data subjects if the risks occur.

Finally, **Part D** contains the mitigating measures that can be taken by either Nextcloud or the individual education organisations to mitigate high or low risks. These measures might either reduce the chance the risks occur, or the impact they might have, or both.

Part A Description of Data Processing

Part A of this DPIA provides an overview of the relevant facts of the data processing via the Nextcloud Enterprise software, as hosted for this DPIA by SURF in its own Amsterdam datacentre. This part starts with a description of the functionalities of Nextcloud Enterprise, and the 5 core services tested for this DPIA.

This part also describes the categories of personal data and data subjects that may be included in the processing; the purposes of the data processing; the different GDPR roles of the involved parties; the different interests related to the tested data processing; the locations where the data are processed, and the retention periods.

Additionally, Part A lists the relevant legal documents that govern the data processing resulting from the use of Nextcloud Enterprise, addresses the applicability of the ePrivacy Directive and includes a separate section on the relevant measures taken by Nextcloud to ensure secure development of the software and secure processing, both by the customer, and by Nextcloud itself (for the limited personal data it receives about the data processing).

A.1 About the Nextcloud Enterprise software

Nextcloud Enterprise is an open-source software suite. Organisations that wish to use this software have to host the software themselves, or look for a third party hosting provider. The software is developed/maintained by the German company Nextcloud GmbH, with the help of external software developers. Nextcloud itself does not offer Nextcloud Enterprise as a cloud service, though it links to partners that can offer the software as fully managed SaaS.[10]

Customers can create text, spreadsheets, mails and presentation files, and collaborate in a shared file and videoconferencing/chat platform with the Nextcloud Enterprise software.

The Nextcloud Enterprise Hub licenses include six main software bundles:

1. Files (filesharing)
2. Groupware (email, calendar, contacts and deck)
3. Talk (videoconferencing and chat)
4. Nextcloud Office (tested with Collabora Online)
5. Nextcloud Assistant (out of scope, LLM only tested as part of Talk)
6. Nextcloud Flow (out of scope)

End users can access the different Nextcloud software bundles via a web interface, using any recent web browser.[11] SURF tested with Mozilla Firefox on Windows and on MacOS (for the admin). SURF did not test the Nextcloud applications on mobile devices.

[10] Nextcloud Partners, URL: https://nextcloud.com/partners/ (last visited 12 April 2026).
[11] Nextcloud user manual, Web Interface, URL: https://docs.nextcloud.com/server/latest/user_manual/en/webinterface.html (last visited 26 January 2026).

SURF tested Nextcloud **Office** with the open source Collabora Online document editing and collaboration software.[12] Nextcloud also offers supported access to other office document editing suites, from ONLYOFFICE, Think Free Office and the on-premises Microsoft Office.[13] The Collabora Online suite (developed by the UK company Collabora[14]) in turn is based on the (desktop) LibreOffice open source software.[15] Different from the Do It Yourself consumer-oriented approach from LibreOffice, both Nextcloud and Collabora offer professional support to organisations and enterprises.[16] Nextcloud CEO Frank Karlitschek explained why Nextcloud did not develop its own Office software, but has chosen to include the Collabora Online software: "*Office suites are super complicated to develop, so it would be impossible to do this without a partner like Collabora Online.*"[17]

The core of Nextcloud Enterprise is the self-developed Nextcloud **Files**. Without Files users would not be able to run Office. Additionally, Nextcloud has developed **Groupware and Talk**, to enable organisations to organise the workflow in a single platform, including mail, shared file storage and videoconferencing/chat functionalities. The detailed data processing functionalities are described in Sections A.1.2.1 to A.1.2.4. The Nextcloud Hub includes two more tools: Flow and the AI Assistant, but SURF only tested AI-functionality in combination with Talk.

Education organisations can purchase Nextcloud Enterprise end user licenses. With such licenses the admins of organisations have (direct) access to Nextcloud engineers. The licenses provide Enterprise customers with security support. Nextcloud writes that it helps Enterprise customers identify and address vulnerabilities and harden servers to protect the safety and integrity of the data on the Nextcloud server.[18] This doesn't mean Nextcloud engineers have access to the self-managed software.

Nextcloud offers three standard Enterprise license plans: Standard, Premium and Ultimate. These plans only cover the use of Nextcloud Files. Customers have to pay for the use of Nextcloud Talk, Groupware and Office as add-ons. The software can be used on mobile and desktop clients, and includes standard enterprise facilities such as SAML Authentication, Windows Network Drive support, password policies, audit logging and workflow handling. The main difference (besides pricing) between the different license plans is that the Ultimate subscription (tested by SURF for this DPIA) offers faster/multi-channel support.[19]

Other benefits for paying customers are lifecycle management and prioritised handling of critical issues (SLA response time of 1 working day, with a two day resolution target).[20] Enterprise customers are prioritised in the communication about security issues: they receive alerts approximately 4-6 weeks before the non-paying community.

[12] Collabora Online, URL: https://www.collaboraonline.com/ (last visited 9 January 2026).
[13] Nextcloud reply to part A of this DPIA, 2 April 2026.
[14] Collabora, About us, URL: https://www.collabora.com/about-us/ (last visited 20 January 2026).
[15] Collabora, The world's premier Open Source office suite – ready for business, URL: https://www.collabora.com/about-us/open-source/open-source-projects/libreoffice.html (last visited 20 January 2026). Collabora explains: "*Collabora, is the driving force behind putting LibreOffice in the Cloud, providing a range of products and consulting to enterprise and government.*"
[16] Collabora Online, Engineering Support, URL: https://www.collaboraonline.com/engineering-support/ (last visited 9 January 2026).
[17] Nextcloud & Collabora Online Success Stories, URL: https://www.collaboraonline.com/partners/nextcloud/ (last visited 9 January 2026).
[18] Nextcloud Enterprise FAQ, answer to the question 'What does the subscription give me?, URL: https://nextcloud.com/faq/ (last visited 26 January 2026).
[19] Nextcloud Enterprise Pricing, URL: https://nextcloud.com/pricing/
[20] Reply Nextcloud to security questions SURF, 18 September 2025, row 23 and 24.

Both Enterprise Premium and Ultimate customers can ask for consulting for custom capabilities. Nextcloud writes: "*Nextcloud consulting goes beyond technical expertise, offering strategic advice for organizations. We analyze your challenges and help you implement a comprehensive, cost-effective and compliance-aware solution which reduces complexity and risks while delivering the highest security and privacy protection*."[21]

A.1.1 Scope of this DPIA

To help education organisations compare the results of this DPIA with previous DPIAs performed for SURF and the Dutch government on Microsoft Office[22] and Google Workspace[23], SURF tested the data processing by the 6 most frequently used Nextcloud work productivity applications:

1. Mail (including Calendar)
2. Write (as part of Nextcloud Office)
3. Present (slides)
4. Spreadsheet
5. Files (data sharing)
6. Talk (with generative AI functionality to transcribe speech to text, whiteboard and polling).

This DPIA applies exclusively to the Nextcloud Enterprise software (not to consumer or community edition freely downloadable versions). The codebase for the different target audiences is the same. Having an Enterprise subscription is not necessary to run Nextcloud services. The key difference between the freely downloadable and the paid Enterprise licenses is the additional support for business customers.[24]

The scope of the DPIA includes the necessary server software:

- The Collabora online server software
- The Nextcloud server environment (6 core software and two selected official apps, namely whiteboard and polling)
- The tested Nextcloud clients (Windows and MacOS desktop)
- Communication with Nextcloud, including a support request.

[21] Idem.
[22] SURF, Results of Data Protection Impact Assessment (DPIA) on Microsoft OneDrive, SharePoint and Teams, URL: https://www.surf.nl/en/results-of-data-protection-impact-assessment-dpia-on-microsoft-onedrive-sharepoint-and-teams . See also the DPIA published by SLM Rijk for the central Dutch government on Microsoft Office online, on iOS and Android at https://www.rijksoverheid.nl/documenten/rapporten/2020/06/30/data-protection-impact-assessment-office-365-for-the-web-and-mobile-office-apps and the 2022 update about mitigation measures at https://slmmicrosoftrijk.nl/wp-content/uploads/2022/11/20221101-Memo-Toelichting-op-de-getroffen-maatregelen-in-Office365-for-the-Web-and-mobile-Office-apps.doc.pdf.
[23] SURF, Google Workspace (undated overview of all relevant documents), URL: https://www.surf.nl/en/themes/vendor-compliance/google-workspace
[24] In reply to part A of this DPIA Nextcloud added other differences: "*early notifications about security issues, branding/whitelabelling, influence on the roadmap, Enterprise Q&A, Nextcloud Guard, access to specific integrations like the Microsoft integrations from Sendent, certified compliance and GDPR documentation*." Nextcloud, 2 April 2026.

Table 1: Overview test users, OS, browser and desktop applications

User/email	OS	Browser	Desktop application
Sjoera Nas (sjoera.nas@privacycompany.nl)	Windows 11 Business, version 25H2, OS build 26200.7171	Firefox 146.0 (64-bit)	Nextcloud Talk version 2.0.4 Nextcloud Files version 4.0.2
Julian Rill (julian.rill@surf.nl)	macOS Tahoe 26.2	Firefox 146.0 (aarch64)	Nextcloud Talk version 2.0.4 Nextcloud Files version 4.0.2
admin (nextcloud@julianrill.nl)	Same as Julian	Same as Julian	Same as Julian

Out of scope

The assessment excludes the underlying infrastructure hosting layer – in this case, SURF's own data centre in Amsterdam (Watergraafsmeer).

SURF installed the Nextcloud All In One (AIO) package, and followed Nextcloud's guidance to use this with Enterprise licenses. The package included some applications and components not tested for this DPIA. This DPIA is limited to some of the applications and components that are fully supported as part of Nextcloud Enterprise support, but the scope does not include all functionalities or all supported apps.[25] Only the 6 core apps mentioned above are assessed in this DPIA.

In addition, any apps that are not supported by Nextcloud, or other optional or experimental modules, including community or third-party apps, are explicitly excluded from the scope of this DPIA, as well as some apps that are supported by Nextcloud such as Deck.

Within the supported Nextcloud Office software, there are other applications besides the 4 tested apps, related to for example project management (Tasks), simple notes based on Markdown (Text) and a common knowledge database (Collectives). These functionalities are also out of scope of these tests.

Besides offering access via a browser, Nextcloud offers client applications for use on desktops running Linux, Windows and MacOS[26], and apps for Android and iOS.[27] SURF tested the installed Files and Talk applications on Windows and on MacOS, and all tested services via the browser Firefox on Windows and on MacOS. SURF did not test the Nextcloud applications (installed or with browser access) on mobile devices.

[25] Nextcloud, Supported Apps, URL: https://docs.nextcloud.com/server/27/admin_manual/installation/apps_supported.html (last visited 26 January 2026). Admins can see all components that are part of the Nextcloud Hub by running php occ app:list – enabled'.
[26] Nextcloud, Installs, Download for desktop, URL: https://nextcloud.com/install/ (last visited 9 January 2026). There is no desktop application for Groupware.
[27] Nextcloud Features, 'Clients', URL: https://nextcloud.com/features/?filter=Clients (last visited 9 January 2026).

SURF did not test the integration of Nextcloud Enterprise with third party software such as Microsoft or Google services, or integration with object storage from these or other cloud providers, or use of Xwiki.).

Also out of scope are two services included in the 'Ultimate' Enterprise license plan: Nextcloud Assistant and Nextcloud Flow. The Nextcloud Assistant[28] is a generative AI feature that can be integrated with core services in Nextcloud Hub. The Assistant supports several large language models. SURF only tested the AI-feature in Talk to transcribe the audio to a text file, based on an on-premises LLM. Assessing the quality and data protection risks of all generative AI features requires a separate DPIA. Nextcloud told SURF it prioritises development of features such as the AI assistant based on the input from its Enterprise customers.[29]

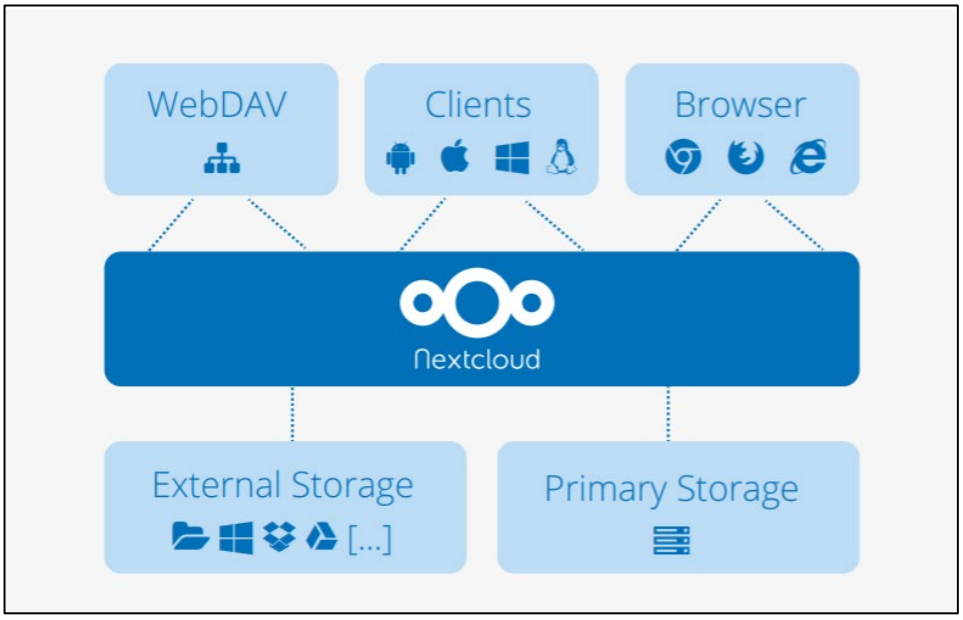
Finally, Nextcloud Flow is out of scope. Flow is a set of automation components that enable organisations to automate and streamline internal workflows. Flow is not part of the standard productivity suite functionality and therefore intentionally left out of scope of this DPIA.

A.1.2 Nextcloud Enterprise products

To test the data processing for this DPIA, SURF procured a Nextcloud Ultimate Enterprise license. Below, the functionalities of the 4 main tested software products are discussed: Office, Files, Talk and Mail/Calendar.

Nextcloud provides a whitepaper about the technical design of its architecture at a high level overview of typical deployment choices.[30]

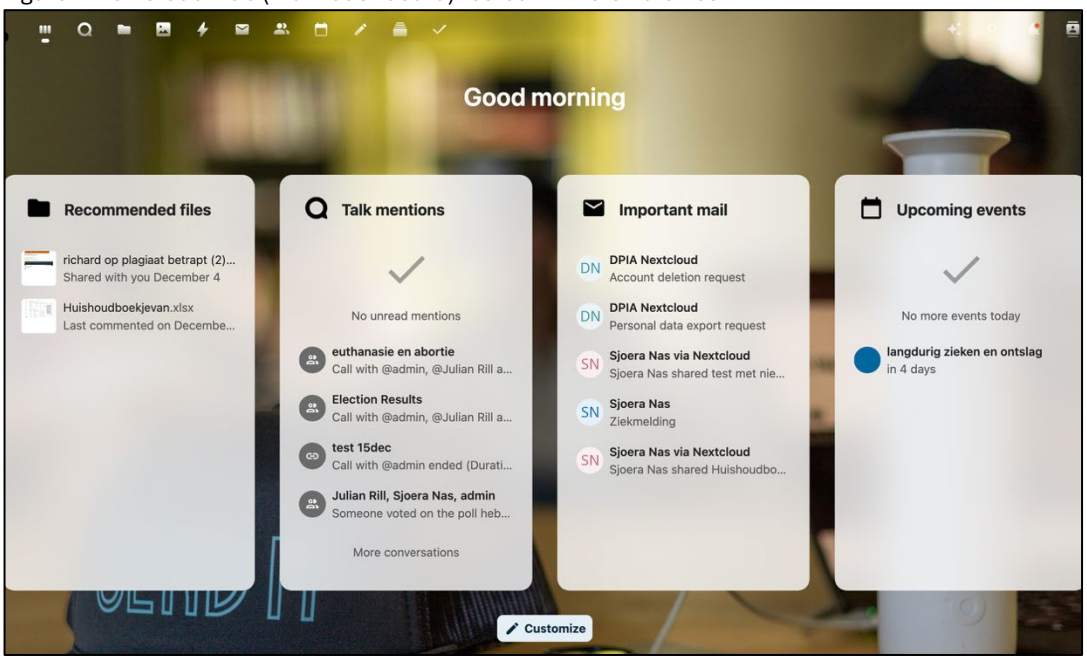
Figure 1: Nextcloud architecture with clients and server set-up[31]



[28] Nextcloud, Nextcloud Assistant, URL: https://nextcloud.com/assistant/ (last visited 9 January 2026).
[29] Input Nextcloud during call with SURF and Privacy Company 12 January 2025.
[30] Nextcloud, Nextcloud Solution Architecture, Bring data back under control of IT, 2018, URL: https://cloud.nextcloud.com/s/fNd8yBwYSo5oDso?openfile=true.
[31] Idem, the paper is available via restricted access download, URL: https://nextcloud.com/blog/whitepapers/architecture-overview/

By default, after logging-in, an end user starts with the Nextcloud Dashboard or Files page. See Figure 2 below. This dashboard provides access to the core Nextcloud Enterprise apps, and offers lists of the most important recent information, such as chat messages, upcoming events and important emails.

Figure 2 Nextcloud Hub (main dashboard) tested in Firefox browser[32]



In this interface, users can:

- Access the available apps, as well as filters and tasks associated with the selected app.
- Use the top navigation bar to create new files, folders and upload files.
- Search for files and entries in the current app.
- Set the current status (Online, Away, Busy, Do not disturb and Invisible, as well as a status message
- Access and change settings:
    - Download desktop and mobile apps
    - Server usage and space availability
    - Password management
    - Name, email, and profile picture settings
    - Manage connected browsers and devices
    - Group memberships
    - Interface language settings
    - Manage notifications
    - Federated Cloud ID and social media-sharing buttons
    - SSL/TLS certificate manager for external storages
    - Two-factor authorisation settings
    - Nextcloud version information[33]

[32] Screenshot made in test set-up 4 December 2025.
[33] Nextcloud user manual, Web Interface, URL: https://docs.nextcloud.com/server/latest/user_manual/en/webinterface.html (last visited 26 January 2026).

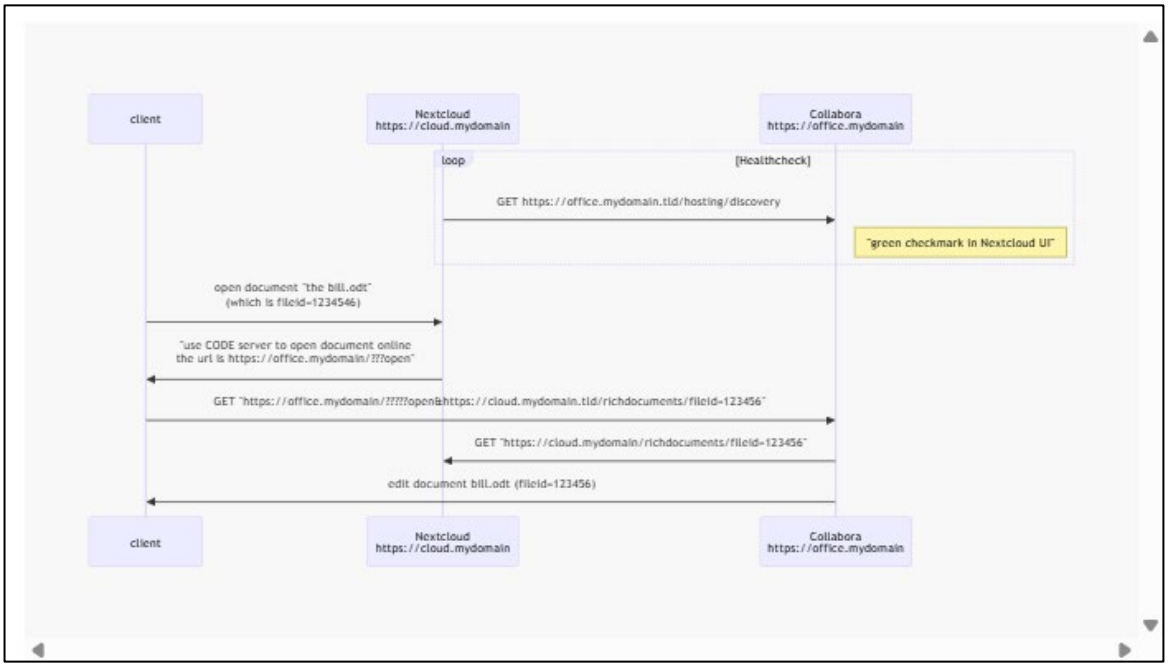
A.1.2.1 Nextcloud Office

Nextcloud Office contains text, numbers, drawings and slides editing software, called Write, Spreadsheet, Draw and Present respectively. Write, Present and Spreadsheet incorporate many industry-standard functionalities and solutions. They for example includes use of templates and styles, options to export to PDF and to edit metadata, as well as a (local) spell and grammar check. See the screenshots later in this Section for the available functionalities.

SURF did not test 'Draw', but used a separate supported app for whiteboard collaboration. SURF tested sharing a virtual whiteboard with participants in a meeting in Talk.

As frontend, Nextcloud Office intensively relies on the Collabora Online backend, also self-hosted by the customer. In a help file, Nextcloud describes the integration as "*not one-way where Nextcloud "pulls" integration from Collabora but it's rather a "communication triangle" between clients, Nextcloud and Collabora, where each component accesses and provides resources from/to another.*" [34]

Figure 3: Nextcloud schema of data traffic exchanged with Collabora Online[35]



[34] Nextcloud Help, Collabora integration guide, undated, https://help.nextcloud.com/t/collabora-integration-guide/151879 (Last visited 26 January 2026).
[35] Idem, screenshot made 27 January 2026.

Figure 4: Editing and sharing options in Write (Windows app) with fictitious CV

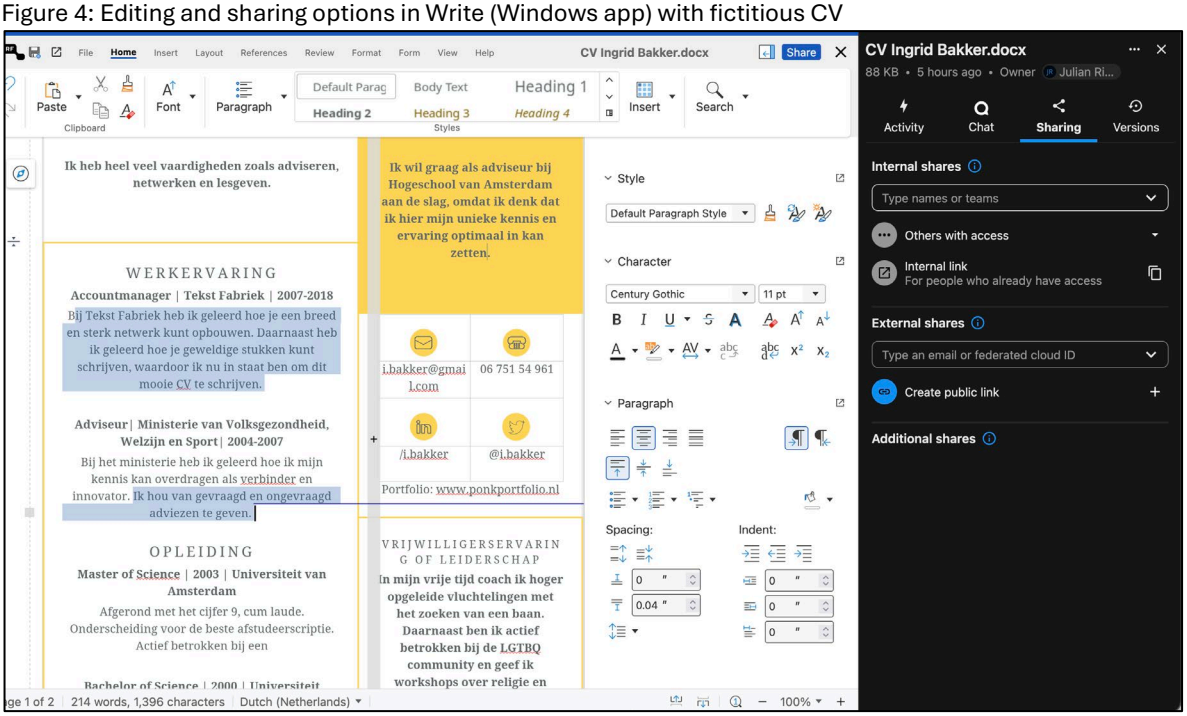
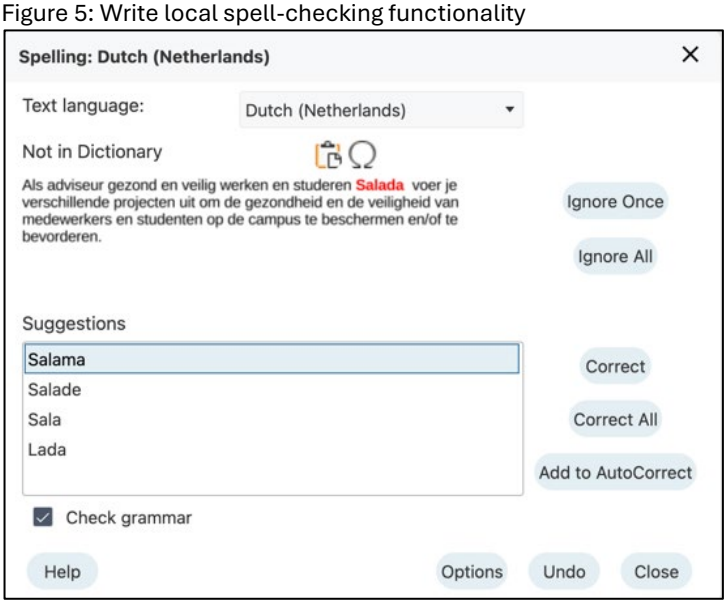


Figure 5: Write local spell-checking functionality



As described in paragraph 2.3 of the Technical Appendix, the collaboration in a document between two users revealed 3 bugs with privacy implications.

- Nextcloud showed different incorrect warnings that a certain action (such as uploading or sending) failed, though the actions were in effect successful.[36]
- The renaming of the document was not effective. The owner/user of the document did not see the new name of the document given by the other user. This was not an incidental error due to perhaps a lag in the connectivity, but consistent behaviour.

[36] In reply to this observation, Nextcloud asked SURF to raise this issue in a support ticket,, or publish via GitHub.

Nextcloud explained this was an intentional feature. Recipients of a share file or folder cannot rename, because that would make it too difficult for the 'owner' to find the document or folder. A recipient can only change folder names if a folder contains multiple documents.

- Nextcloud by default does not include identifying data about the author in the metadata of a document created or opened in Write, even though by default the option 'apply user data' is enabled. The properties of the document did show a total editing time of 50 minutes and revision number 3, while SURF tested with a new document. This may be caused by the fact that the blank document is also a template/dotx. The content didn't change when SURF disabled the option 'apply user data'. In reply to a comment from Nextcloud that it couldn't reproduce this issue, SURF retested 16 April 2026, both in the original test environment and on a fully updated server. Both tests continued to show the same issue.

Figure 6: Metadata example in Write[37]

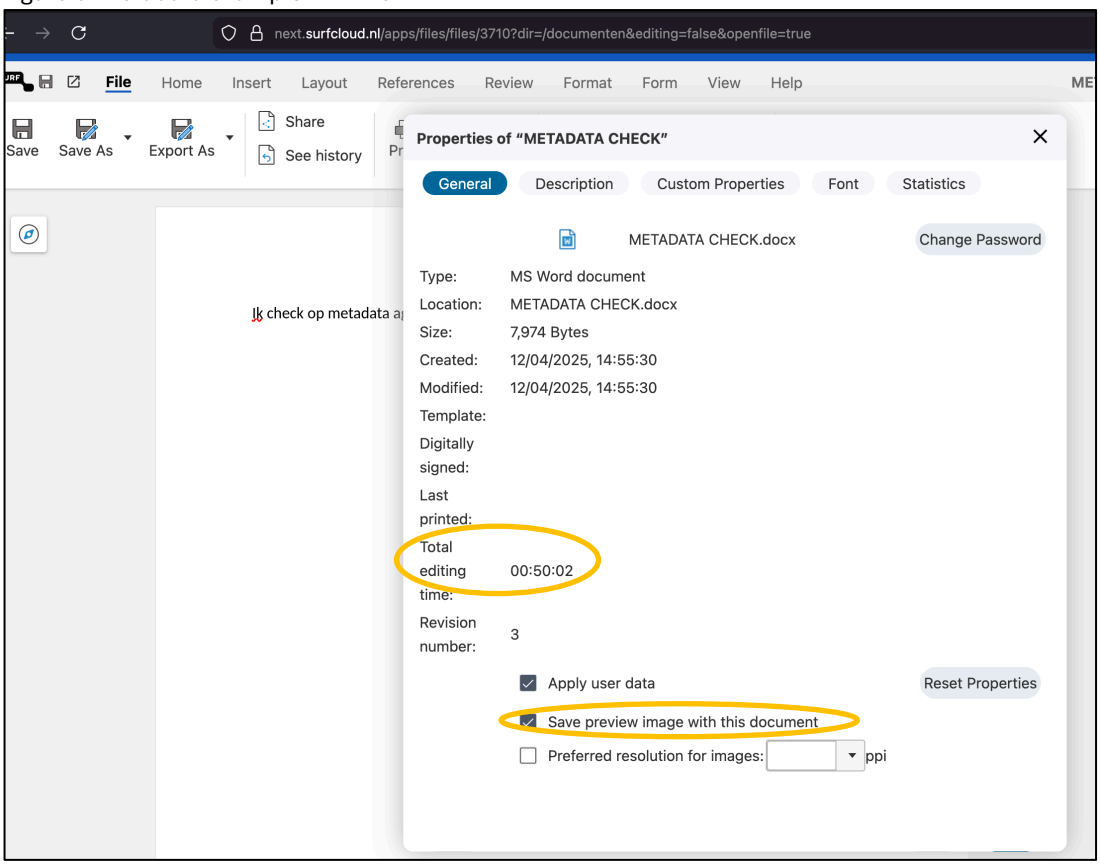
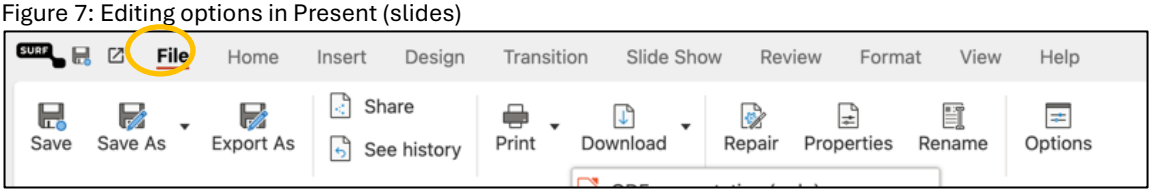


Figure 7: Editing options in Present (slides)



[37] Screenshot taken 4 December 2025 in the SURF test instance, and repeated 16 April 2026 in fully updated environment.

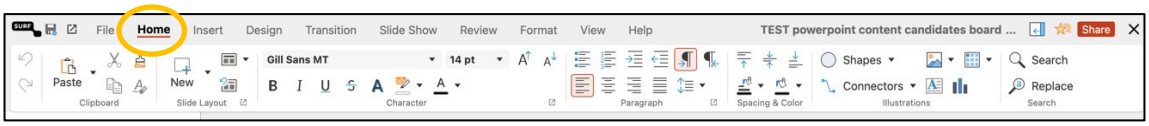
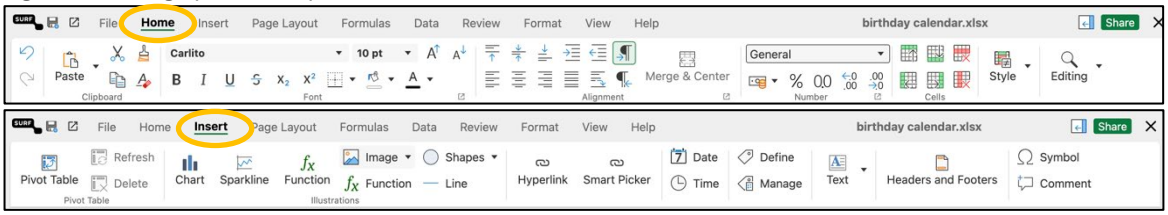


Figure 8: Editing options in Spreadsheet



Nextcloud does not offer a package that completely covers the functionalities of Microsoft SharePoint. Nextcloud offers Collectives[38] , Pico CMS for blogs[39] and Tables[40], but these are out of scope of this DPIA.

A.1.2.2 Nextcloud Files

Nextcloud files is a cloud storage and file sharing software that provides access to sharing and collaboration independent from the time zone or geolocation of the participants.

Nextcloud Files includes access to external storage via FTP, Windows Network Drives, SharePoint and Samba.[41]

With File access control and automatic file tagging admins can set rules for access for specific (groups of) users, or specific geographic regions. This feature enables admins to for example limit sharing of internal data outside of the organisation.[42]

Nextcloud Files also offers File Drop, functionality for users to securely send and receive files, also from external relations that do not use Nextcloud.[43] Nextcloud explains: "*File Drop supports a wide range of storage technologies including NFS, SMB and Windows Network Drive, SharePoint, Object Storage and many more.*"[44] This means end users can easily exchange files with other persons that use Windows or object storage on a cloud hosting provider.

Users can upload a file to a folder in Files, and only share access to that specific file with another person in or outside of the organisation, also for people without a Nextcloud account. Users can share a randomly generated hyperlink (with a random 15-digit token[45]), or create a customized link, with an expiration date and access rights. Users can also choose if they want to exchange a password via mail, or only orally. Other existing content in the folder is automatically hidden from the share recipient. Nextcloud added in reply to this

[38] Nextcloud Collectives, URL: https://apps.nextcloud.com/apps/collectives.
[39] Nextcloud Pico CMS voor blogs, URL: https://apps.nextcloud.com/apps/cms_pico.
[40] Nextcloud App store, Nextcloud Tables, currently version 33, URL: https://apps.nextcloud.com/apps/tables.
[41] Nextcloud Features, Clients, External Storage, URL: https://nextcloud.com/features/#clients.
[42] Idem.
[43] Nextcloud File Drop: convenient and secure file upload and share for Enterprise, 3 February 2026, URL: https://nextcloud.com/blog/file-drop-convenient-and-secure-file-exchange-for-enterprises/.
[44] Idem, section 'Under your control'.
[45] Nextcloud, https://docs.nextcloud.com/server/latest/user_manual/en/files/sharing.html#public-link-shares.

DPIA that it allows users to create multiple links, for example by sharing directly to an email address or by creating *named links* with each different permissions.[46]

File Drop employs industry-standard TLS to encrypt data in transit. Customers can also use server side encryption to encrypt data-at-rest. However, as Nextcloud explains, "*encryption keys will be present in memory of the Nextcloud server during the time a user is logged in and could be retrieved by a determined attacker. We take care to ensure keys are not stored unencrypted on permanent storage and at rest keys are encrypted using a strong cipher.*"[47]

For highly confidential, sensitive or (state) secret data, specific end users may want to deploy encryption with a key that is under their own control, only available on their personal device, on a trusted third party server or offline, and not on the Nextcloud server.

Nextcloud offers End-to-end Encryption client-side (E2EE) for files (in Files) and for calls (in Talk), with apps that are installed on the end user device. Even if a malicious actor manages to breach the (self-hosted) server, the key cannot be copied because the encryption is done with the '*Zero-knowledge proof*' protocol: the participants do not need to convey the secret via the server.[48] Nextcloud explained that it cannot technically offer E2EE for chat content in the browser, as this would inherently break the security E2EE offers, but does reluctantly offer it, because customers ask for it. Generally Nextcloud advises against E2EE because is use prevents functionality like searching in chats.[49]

The availability of E2EE can be useful if the users don't trust the admins of their own organisation, or are afraid that their self-hosted server may be compromised by malicious actors. The use of E2EE can for example be necessary for specific employees that work with confidential information such as members of a Works or Students Council (Medezeggenschaps- or Ondernemingsraad). Or for employees that process state secret information or information that is otherwise likely to attract intrusion attempts from skilled (state) malicious actors. However, these two examples are still edge use cases compared with the necessity to use E2EE for all sensitive personal data processed by a (cloud) provider subjected to foreign (non EU) laws, to protect against the risk that the provider is compelled to disclose personal data to a government authority or intelligence agency in a third country.

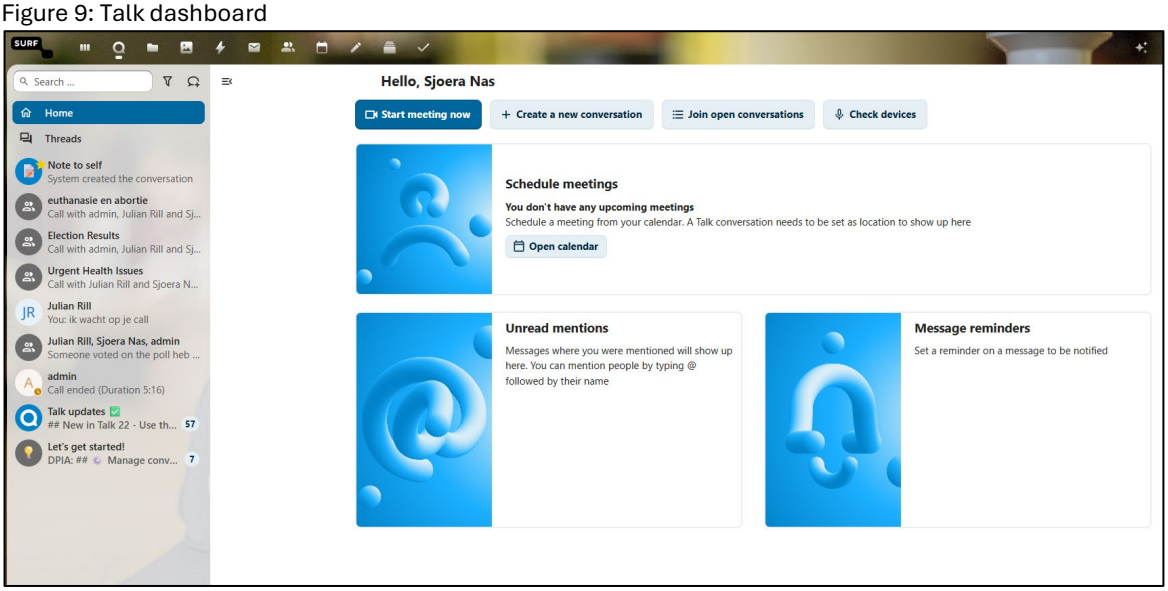
Use of E2EE is not desirable for all personal data processing. As Nextcloud itself also writes, if only the end user can decrypt files, there is a serious risk of loss of personal data if that user loses his or her key. "*While End-to-End encryption is meant to prevent access to data for other parties the reality is: People may lose their encryption keys. While in an home user environment this may be acceptable, in an enterprise this can have grave implications*."[50] That is why Nextcloud recommends Enterprise customers to work with a central data recovery key, not stored on that same instance but for example in a physical vault.

[46] Nextcloud reply to part A of this DPIA, 2 April 2026.
[47] Nextcloud, Encryption and hardening, URL: https://nextcloud.com/encryption/ (last visited 9 January 2026), plus whitepaper End-to-end encryption design, 20 September 2017, only available after providing contact data, URL: https://nextcloud.com/blog/whitepapers/end-to-end-encryption/.
[48] Idem. Wikipedia explains the term 'Zero-knowledge proof' as: "*a protocol in which one party (the prover) can convince another party (the verifier) that some given statement is true, without conveying to the verifier any information beyond the mere fact of that statement's truth*". URL: https://en.wikipedia.org/wiki/Zero-knowledge_proof (last visited 9 January 2026).
[49] Nextcloud reply to part A of the DPIA, 2 April 2026.
[50] Nextcloud whitepaper End-to-end encryption design, p. 3.

A.1.2.3 Nextcloud Talk

Nextcloud Talk[51] is the tool for text chat, video calls and webinars. Talk enables users to have one-on-one conversations or group meetings. Talk can show chronological or threaded conversations. All scheduled meetings, messages, mentions and scheduled reminders are shown in the Nextcloud Talk Dashboard.

Figure 9: Talk dashboard



If organisations allow users to share files with external users via Talk or Files, admins can take two measures to protect the files:

1. adding a watermark to help prevent unauthorised copying (not tested by SURF) and
2. make it harder for participants to download by hiding the download button.

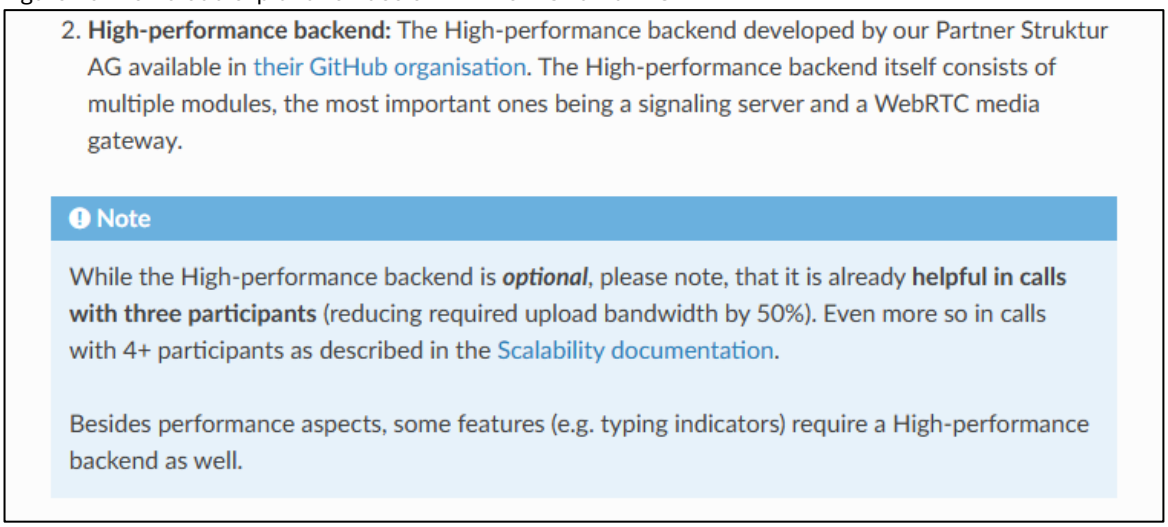
Nextcloud Talk supports federated collaboration. The software gives the option to join group chats on another Nextcloud server and use many of the core features. It is also possible to organise audio and video meetings across different Nextcloud Hubs (to meet colleagues from another faculty or institution, or maybe a partner who is using Nextcloud too.)

As mentioned above, Nextcloud Talk also supports end-to-end encrypted calls for sensitive communication, through mobile apps and desktop clients.

Organisations can also enable users (both colleagues and external participants) to participate by phone, if they set-up their own SIP server, and the High Performance Backend developed by the German company Struktur AG.[52] Nextcloud explains this software is optional, but factually indispensable for a good video quality. See Figure 10 below. SURF did not test the SIP bridge.

[51] Nextcloud Talk, URL: https://nextcloud.com/talk/ (last visited 26 January 2026).
[52] See GitHub support discussion about the SIP configuration, URL: https://github.com/nextcloud/spreed/issues/5370#issuecomment-798400645 (last visited 26 January 2026). See also Nextcloud High Performance Backend for Talk on Nextcloud with Docker, URL: https://help.nextcloud.com/t/high-performance-backend-for-talk-on-nextcloud-with-docker/215828 (last visited 26 January 2026).

Figure 10: Nextcloud explanation use of HPB from Struktur AG[53]


2. **High-performance backend:** The High-performance backend developed by our Partner Struktur AG available in their GitHub organisation. The High-performance backend itself consists of multiple modules, the most important ones being a signaling server and a WebRTC media gateway.

Note

While the High-performance backend is ***optional***, please note, that it is already **helpful in calls with three participants** (reducing required upload bandwidth by 50%). Even more so in calls with 4+ participants as described in the Scalability documentation.

Besides performance aspects, some features (e.g. typing indicators) require a High-performance backend as well.

To invite external chat participants users can share a URL to public rooms on the Nextcloud server. The chat remains open even when the user leaves a call, but admins can set retention periods.[54] See Sections 4 and 11 of this DPIA for privacy controls and retention periods.

In the test set-up, SURF choose to include **3 optional features** in Talk, to better reflect usage wishes from education organisations and end users.

1. Generative AI to transcribe speech to text
2. Whiteboard
3. Polling

Transcription of meeting with genAI
Organisations can only use the tested AI-feature in Talk for transcriptions if they install an *on-premises* language model on their own server.[55] This requires a server with a high compute capacity.[56]

SURF tested the AI functionality in Talk by recording and transcribing three conversations about imaginary health and gender issues between a fictive employee and a fictive manager, two conversations in English and one in Dutch. The transcription was done by the on premises LLM Whisper from OpenAI. SURF installed Stt_whisper2. Since December 2025, Nextcloud allows Enterprise customers to download the Whisper large-v3-turbo model in the Enterprise license, described as "*Ships with Whisper large-v3-turbo model (similar quality as large-v3, but 5-8 times faster).*"[57]

[53] Nextcloud Talk, Quick Install, URL: https://nextcloud-talk.readthedocs.io/en/latest/quick-install/ (screenshot made 26 January 2026).
[54] Nextcloud, File Sharing (user manual), URL: https://docs.nextcloud.com/server/latest/user_manual/en/files/sharing.html (last visited 26 January 2026).
[55] GitHub, Nextcloud Assistant, URL: https://github.com/nextcloud/assistant
[56] SURF tested with a single Nvidia GeForce RTX 2080 Ti for local AI processing compute.
[57] GitHub, Nextcloud sst-whipser2 Change Log, URL: https://github.com/nextcloud/stt_whisper2/blob/main/CHANGELOG.md (last visited 1 February 2026).

As explained in more detail in the Tech Appendix, the transcriptions did not distinguish between the contributions of the two participants, and did not include their names (other than in the transcribed content of the conversation). The transcriptions in English were fairly accurate, except for a few mistakes. The transcription in Dutch however was a lot less accurate than the two English conversations, as highlighted in the Tech Appendix.

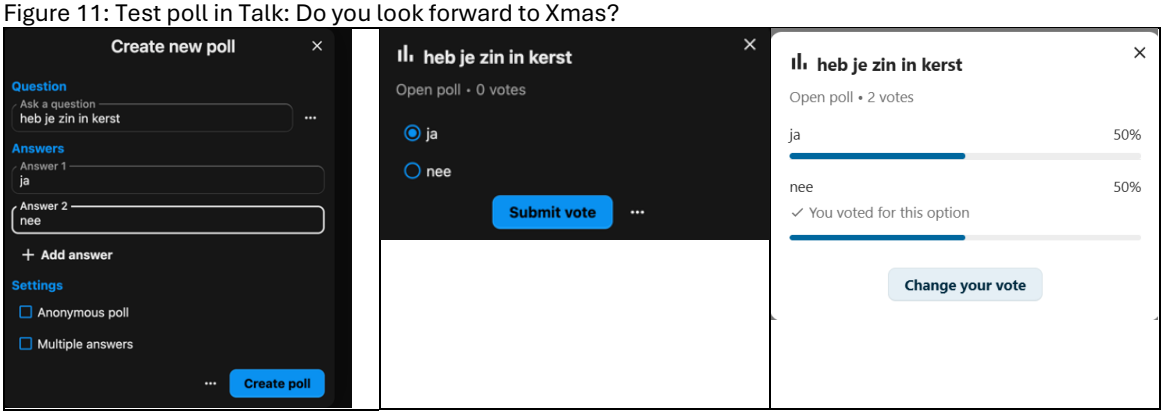
None of the transcriptions showed any apparent bias in transcribing the dialogue about health and gender issues. This is relevant in view of academic large scale tests that showed bias in OpenAI's most frequently downloaded Whisper Large-v3 model, released in November 2023.[58]

At the end of every transcription, Nextcloud shows the following warning sentence: *Transcript is AI generated and may contain mistakes*.

Polling in Talk

SURF tested the polling feature with two participants and the question '*Do you look forward to Xmas*?'. 50% (i.e. 1 participant) answered Yes and 50% (the other participant) answered No.

Figure 11: Test poll in Talk: Do you look forward to Xmas?



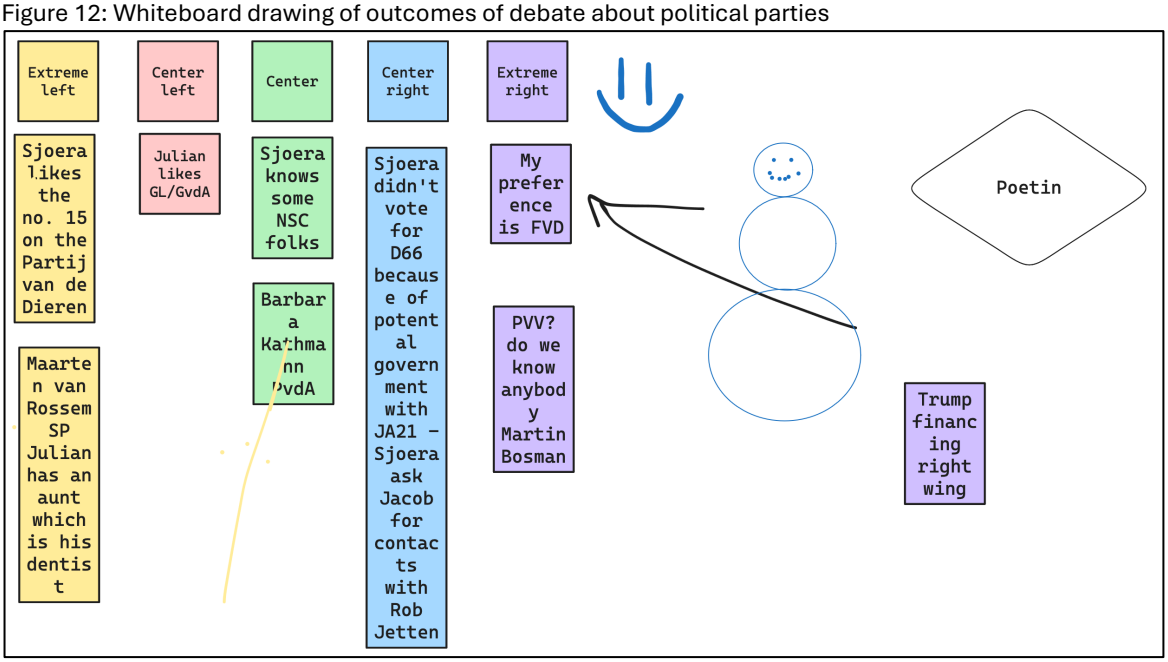
The poll results do not include names or IP addresses of the participants. However, in the tested case the poll was not 'anonymous' as Nextcloud suggests, but pseudonymous, because the host could see the result from the other known participant. Nextcloud replied that it should be obvious that the poll is not anonymous in case of two participants, but it does consider the results anonymous of any poll in which 3 or more people participate. This legal point of view will be addressed in Section A.2.2.1.

Whiteboard in Talk

SURF tested the supported Whiteboard collaboration app in Talk by organising a (fictitious) discussion about election results in the Netherlands, and taking notes of the comments of the two participants on the Whiteboard. SURF used this extreme test scenario to be able to better detect traces of the content in the available logs.

[58] AP, Researchers say an AI-powered transcription tool used in hospitals invents things no one ever said, 26 October 2024, URL: https://apnews.com/article/ai-artificial-intelligence-health-business-90020cdf5fa16c79ca2e5b6c4c9bbb14.

Figure 12: Whiteboard drawing of outcomes of debate about political parties



A.1.2.4 Nextcloud Mail, Calendar, Contacts

Nextcloud Groupware[59] integrates Mail, Calendar and Contacts, and other productivity features such as Deck (out of scope of this DPIA). Users can transform chat messages into tasks, show task deadlines in Calendar and attach files to a task from the sharing dialog.

Nextcloud does not include a mail server– education organisations have to separately configure a mail server (for example, Stalwart or Dovecot Pro).[60] Nextcloud Mail is a client for IMAP-infrastructure. Mail offers all common mail functionalities, including support for multiple accounts, creation of group mail boxes and calendar integration. Mail includes indispensable features such as search, filtering (if the admin has configured a Sieve server), the choice between threaded or chronological view, out-of-office messages, quick actions in emails to handle tasks, mark emails as read, quick actions, such as moving mails to a project folder.

Nextcloud also offers a *Priority Inbox* feature, to sort messages as *Important* or *Others*, based on machine learning of most frequent contacts with a person. This feature does not involve the use of a (self-hosted) LLM but uses the metadata about most recent interactions to train a neural network. SURF did not have enough test mails to test the (local) algorithm's correctness. The Nextcloud software puts the first 30 mails in the 'Priority' column, and only starts to 'learn' from user feedback after those first 30 mails.[61]

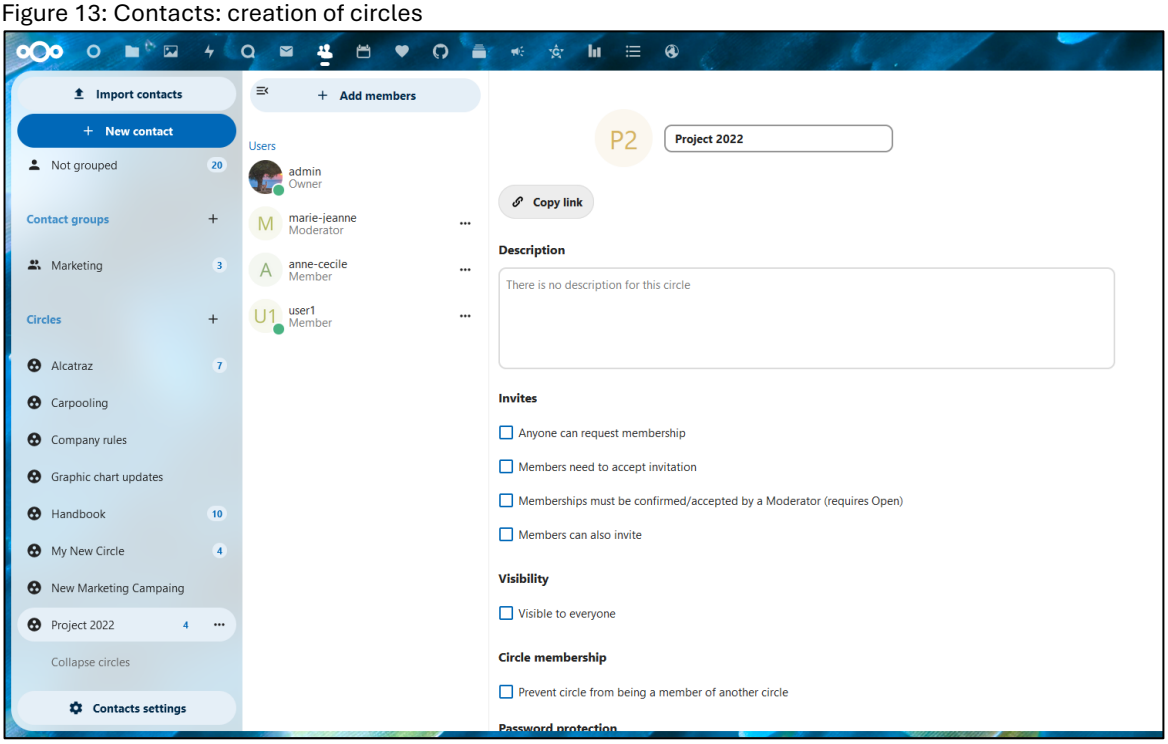
Admins can also enable some generative AI-features such as AI summary, smart replies and translations, but these features were out of scope of this DPIA.[62]

[59] Nextcloud Groupware, URL: https://nextcloud.com/groupware/ (last visited 26 January 2026)
[60] Nextcloud, admin configuration Email, URL: https://docs.nextcloud.com/server/stable/admin_manual/configuration_server/email_configuration.html (last visited 12 April 2026).
[61] GitHub, Nextcloud Mail, Behavior of 'Priority Inbox', URL: https://github.com/nextcloud/mail/issues/3293 (discussion closed July 2021).
[62] Nextcloud user manual, Using the Mail app, URL: https://docs.nextcloud.com/server/latest/user_manual/en/groupware/mail.html (last visited 26 January 2026).

Users can create meeting proposals in Nextcloud Calendar, including a video call in Talk. They can add team members or external participants, track availability, pick slots and let the attendees vote on the meeting time. They can also attach files to a calendar invite. Nextcloud explained it helps admins prevent oversharing of files with security rules. There are two ways of attaching a document: users can share a link via Files, or attach a document to mail. If users share a link, they can apply security rules for access with the options for folders in Files: *allow downloads* or *remove download*. In the latter case the recipient has read-only access. Nextcloud also explained it does not yet offer a (systematic) solution such as labelling of documents to prevent users from (accidentally) oversharing through attached documents.

Nextcloud Contacts offers an option to create user groups, called 'Circles' when tested, but since renamed in 'Teams'. Nextcloud explains that users can choose to share files and folder or Talk conversation with their circles (now: Teams).[63] This can be a useful feature for collaboration between teachers, or for online teaching.

Figure 13: Contacts: creation of circles



A.2 Legal: personal data and enrolment framework

This section provides an analysis of the legal conditions that govern the data processing based on the contract between SURF and Nextcloud. This section also provides a general legal description of the categories of personal data and data subjects, to help the education organisations identify the data they will process with Nextcloud as well as the relevant data subjects.

[63] Nextcloud user manual, Using the Contacts app, URL: https://docs.nextcloud.com/server/31/user_manual/en/groupware/contacts.html (screenshot made 26 January 2026).

The next section A.3 provides a description of the technical findings on the personal data processing, as for example collected in log files.

A.2.1 Definition of personal data

According to Article 4 (1) (a) GDPR,

"'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

In the framework contract, Nextcloud uses the definition of Customer Data for the data it processes as processor. Nextcloud describes Customer Data in its Terms and Conditions, and describes its role as processor for the personal data in Customer Data, as defined in Article 4(2) of the GDPR.[64] Nextcloud's term *Customer Data* only refers to the contents of support tickets, including attachments uploaded by admins, but does not include the metadata Nextcloud can collect outside of support tickets. In its standard Data Processing Agreement, Nextcloud defines the scope of the agreement as "*processing of personal data as specified in Annex I*."[65] The Annex contains an overview of the categories of personal data Nextcloud processes as processor, limited to support tickets and log files submitted through support tickets:

- *First and last name*
- *Email address*
- *Information submitted through* ***support tickets, including log files and system reports*** *that may incidentally contain:*
    - *Usernames or user IDs*
    - *IP addresses*
    - *File names or metadata*
    - *Timestamps*
    - *Other technical identifiers or diagnostic data*

To help education organisations perform their own DPIA, Section A.2.2 below contains a description of categories of personal data whose processing has a different impact on data subjects, and are therefore relevant for this risk assessment. This DPIA distinguishes between 5 categories of personal data:

1. Content Data (called Customer Data by Nextcloud, only available to customers within the self-hosted software)
2. Account Data, in two types:
    a. admin Account Data
    b. Contact Data from procurement officers
3. Diagnostic Data, in three types:

[64] Nextcloud Terms and Conditions, version 3.8 (19.12.2025), URL: https://cloud.nextcloud.com/s/EwNz7GxbSKXKNpb, Article 4 – Data Protection.
[65] Annex I however, only contains the names of the signing parties. Nextcloud has explained in reply to part A of this DPIA it will correct this numbering mistake in the next version of the T&C

   a. Logs only available to customers
   b. Logs optionally shared by customers with Nextcloud GmbH
   c. Logs created by Nextcloud GmbH
4. Support Data (both the contents of support tickets and metadata)
5. Website Data, in two types:
   a. the restricted access websites, i.e. the admin and support portal, and
   b. the publicly available nextcloud.com pages with relevant technical documentation, DSAR form and legal information..

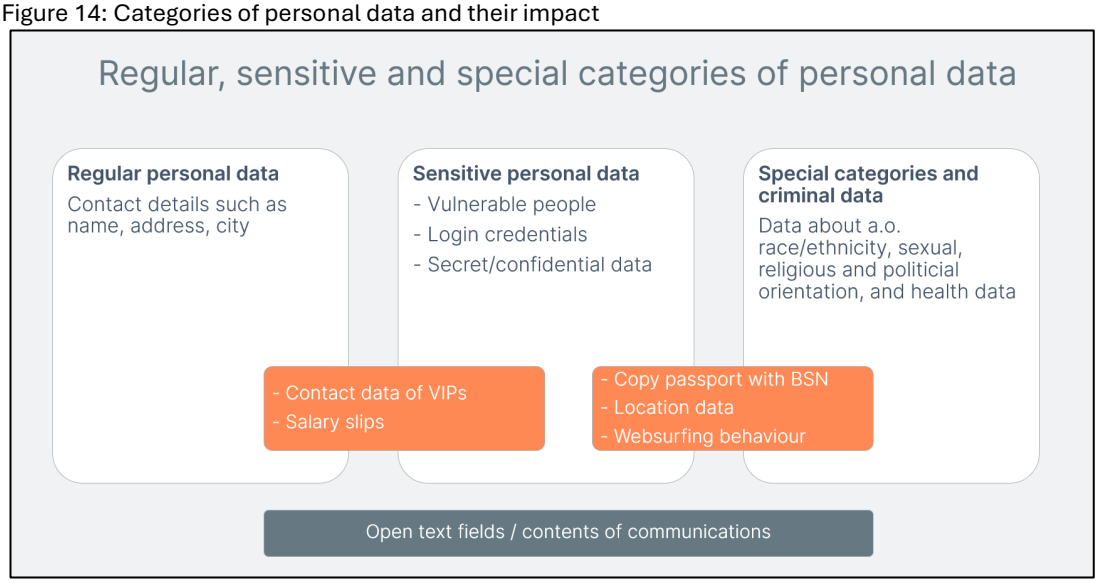
Section A.2.2.4 below similarly provides a high-over description of the different kind of persons involved by the data processing, the data subjects.

A.2.2 Categories of personal data in the Content Data

Different from cloud providers, the company Nextcloud generally does not collect any Content, Website or Account Data. Because the software is self-hosted, such personal data are only collected by the customers (education organisations) themselves. However, to help education organisations perform a DPIA on the Nextcloud data processing, this DPIA also addresses the risk of the processing of personal data by the organisations themselves.

This section first provides a general description of the types of personal data that can be processed as a result of the use of Nextcloud Enterprise, distinguished in the impact of the processing on data subjects (confidential, sensitive and special categories of data). As shown in Figure 14 below, there are no hard lines between the categories. Depending on the context, the same data may be regular, sensitive or special categories of data.

Figure 14: Categories of personal data and their impact



This section with a general description of possibly sensitive data is followed by a specific description of the actual Content, Account, Diagnostic, Support and Website Data created and processed in the test setup.

A.2.2.1 Confidential and Classified information

The Dutch government defines 4 classes of Classified Information, ranging from confidential within the ministry to extra secret state secret. Education organisations (employees and students) can also process such Classified Information.

Classified Information is not a separate category of data in the GDPR or other personal data legislation. Nonetheless, information that is qualified as classified information, whether it qualifies as personal data or not, must legally be protected by special safeguards. The processing of this information can also have a privacy impact when it is related to an individual. If the personal data of an employee, such as an account ID, or unique device identifier, can be connected to the information that this person works with Classified Information, the impact on the private life of this employee or even student may be higher than if that person would only process 'regular' personal data. Unauthorised use of this information (if there is a data breach on the self-hosted environment) could for example lead to a higher risk of being targeted for social engineering, spear phishing and/or blackmailing.

If employees share access to such confidential documents stored in Nextcloud Files, they can inadvertently cause data breaches if unauthorised people can access the contents. Nextcloud offers tooling to tag documents and restrict access but implementation of such tools requires a lot of time and endurance. Many file storage servers are notoriously filled with outdated data because there is no natural incentive to clean up data, such as costs or degradation of service quality.

Another example of confidential data is the results of polls, for example if the polling tool is used for internal elections, such as for the medezeggenschapsraad (Participation Council), or to assess the quality of a teacher. As described in Section A.1.2.3, Nextcloud does not enforce a minimum threshold to show polling results, as it maintains all results with 3 or more participants are anonymous. As will be discussed in Section 0, Nextcloud does not offer audit logs about polls, and the poll results itself do not include names or IP addresses of the participants. These are good technical measures to minimise the risk of identifiability, but they do not prevent relatively simple identification if two of the three participants make their vote / input known, or reidentification of participants if the poll refers to a document while all identifiable access to that document is logged.

A.2.2.2 Personal data of sensitive nature

Some types of 'normal' personal data have to be processed with extra care, due to their sensitive nature. Examples of such sensitive data are contents of communication, web surfing behaviour, financial data, traffic and location data. The metadata about communication (in this case personal data exchanged via Files, Talk and email) are also of a sensitive nature, as they reveal many personal characteristics about an individual.

The EDPS explains in its guidelines on the use of cloud computing services by European institutions that special categories of data should be interpreted broadly when interpreting the risks for data subjects. The EDPS writes:

"*Nevertheless, this is not the only factor determining the level of risk. Personal data that do not fall under the mentioned categories might lead to high levels of risk for the rights and*

freedoms of natural persons under certain circumstances, in particular when the processing operation includes the scoring or evaluation of individuals with an impact on their life such as in a work or financial context, automated decision making with legal effect, or systematic monitoring, e.g. through CCTV."[66]

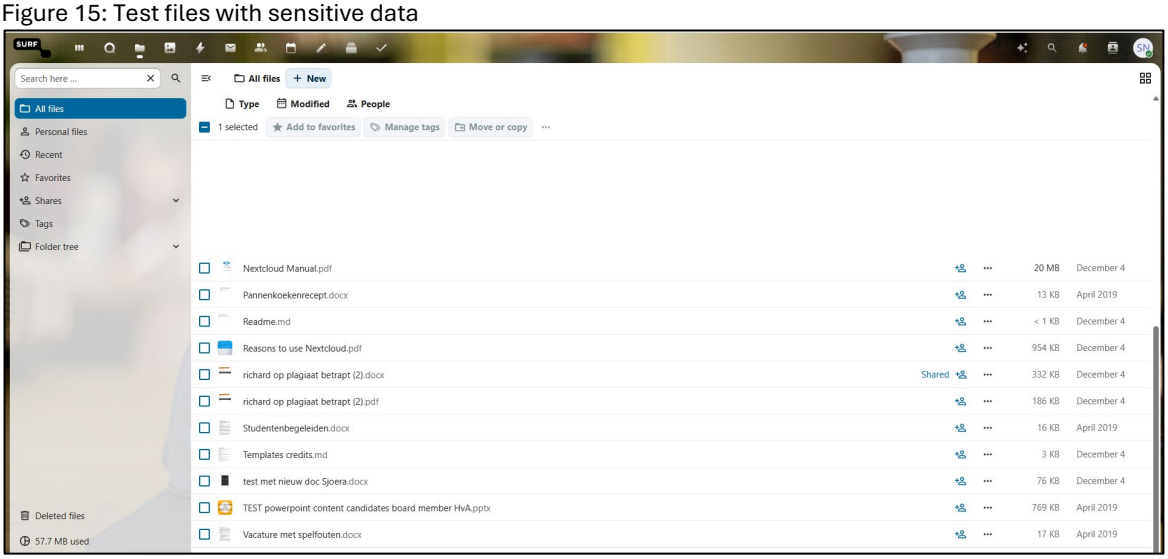
The EDPS also refers to the criteria provided by the Article 29 Working Party when a Data Protection Impact Assessment (DPIA) is required.[67]

The sensitivity of the data is thus related to the level of risk for the data subjects in case the confidentiality of the data is breached. Even home addresses and telephone numbers can be sensitive, for example from professors with controversial opinions that may fear intimidation or worse at their home address. Credentials from admins are another example, as they may become targets of spear phishing, social engineering or blackmail to obtain access to larger amounts of personal data via them.

Risks may vary from slight embarrassment if the employer notices from the log files that an employee has for example used a specific Nextcloud Enterprise feature very frequently, to a chilling effect if the employer does not specifically exclude the use of the log files for performance assessments, to exposure of VIP data (including for example professors or foreign guests) that may unintentionally be accessible for an employee (if an organisation makes mistakes with authorisations, and allows all employees to access a folder with personal data on Nextcloud Files).

It is likely that many employees and students process personal data of a sensitive nature about colleagues and other data subjects on a daily basis, in their File folders, in emails and as shared in Talk.

Figure 15: Test files with sensitive data



The variety of sensitive data that organisations can process with Nextcloud Enterprise cannot be overestimated. In the test scenarios developed for this DPIA examples were used

[66] EDPS, Guidelines on the use of cloud computing services by the European institutions and bodies, 16 March 2018, p. 11, URL: https://www.edps.europa.eu/sites/default/files/publication/18-03-16_cloud_computing_guidelines_en.pdf.
[67] Idem.

of an email with health information (ziekmelding), a fictitious criminal record about a truant (spijbelaar), a CV, a job application, an assessment of candidate board members and financial data about personal expenses. See Figure 15 above. Names of such files can become part of the audit and activity logs.

A.2.2.3 Special categories of personal data

Based on the GDPR, the processing of special categories of personal data is prohibited, unless one of the exceptions from the limitative list included in the GDPR applies.

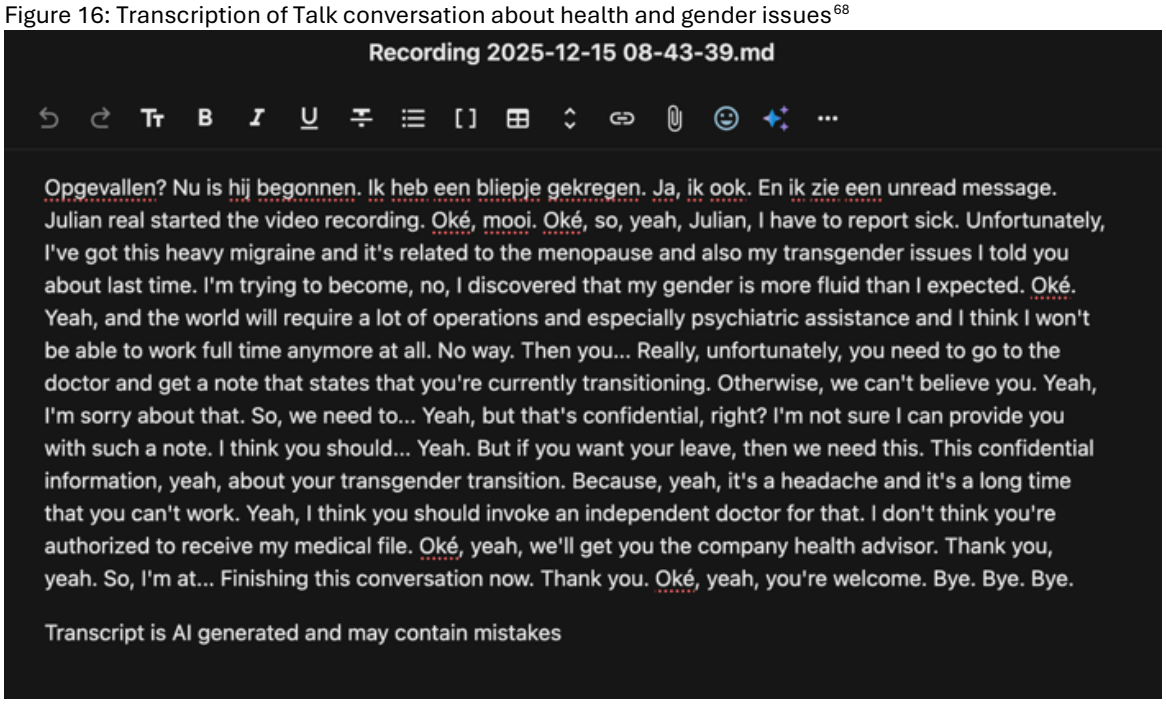
According to Article 9 (1) GDPR, personal information falling into special categories of data are any:

"*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*".

With special categories of data, the principle is one of prohibition: special data may not be processed. There are exceptions to this rule, however, for instance when the data subject has explicitly consented to the processing, or when data have been made manifestly public by the data subject, or when the processing is necessary for the data controller to exercise legal claims.
Education organisations can process any special categories of personal data with the self-managed Nextcloud Enterprise software, as part of Content Data in emails, files or chats, but also when students or employees collect or analyse special categories of data for research purposes.

For testing purposes, SURF set up a (fictive) dialogue about politics, with a whiteboard with the names of political parties. During this meeting, participants provided input on the whiteboard with their opinion or knowledge of party members. See Figure 12 above. SURF also tested the transcription of a dialogue in Talk about all kinds of health and gender issues. See Figure 16 below.

Figure 16: Transcription of Talk conversation about health and gender issues[68]



A.2.2.4 Possible categories of data subjects

This umbrella DPIA can only indicate types of personal data and types of data subjects that may be involved in the processing, but cannot assess the specific risks of the actual data processing for each organisation that will use Nextcloud Enterprise. The risks for data subjects strongly depend on the privacy choices and settings that each organisation makes, as well as on the nature of the work performed by their employees and students/pupils.

This DPIA uses the term ‘employee’ to describe a broad group of workers, regardless of their contracting situation as internal, temporary or external employees, and including employees that perform technical administration tasks (admins). Similarly, the term ‘students’ refers to all persons that follow educational programs from SURF members, and are assigned a login account for access to Nextcloud Enterprise.

Employees’ and students’ use of Nextcloud Enterprise is recorded in local log files. These data are only accessible for the (admins of the) customers themselves, and stored locally for a period of time initially determined by Nextcloud. Organisations themselves can export the logs and determine to retains these logs for shorter or longer periods of time. The audit log can contain information about former employees, if organisations do not anonymise such data by deleting individual credentials or by removing data relating to a specific person from log files. The different logging options are discussed in Section A.3.3 below.

A.2.3 New Data Processing Agreement SURF and Nextcloud

Nextcloud does not apply an Acceptable Use Policy, as it does not host any data itself, and hence, cannot impose usage restrictions.

[68] The transcription did not include the names of the participants, or otherwise separate the participants.

Nextcloud's Enterprise **Terms and Conditions** mostly regulate the type of support Nextcloud provides, only third level support. The terms include a brief section on data protection. In this section Nextcloud asserts that it does not require any personal data of Customer for the provision of support services.

"*NEXTCLOUD does not require any personal data of CUSTOMER for the provision of the support services defined in this agreement. It is the responsibility of the CUSTOMER to protect its data and to ensure that data is not transmitted to NEXTCLOUD.*"[69]

The statement is incorrect because all support communication between a customer and Nextcloud inevitably is personal data, even though Nextcloud does not aim to collect directly identifiable data. If an admin from a customer contacts Nextcloud for third line support, Nextcloud processes contact data. The support ticket includes personal data relating to the admin (at the minimum level, a pseudonymous mail address like admin@customer.nl), the IP address and an identifier relating to the customer license). Additionally, the contents of the support request can include personal data from other people. Even if an admin only asks for help with a technical update issue, the whole correspondence has to be qualified as personal data, since it relates to an activity of that identifiable admin. For SURF-members this statement is overruled by the explanations about personal data processing in the amended DPA.

The Terms and Conditions also contain a provision on license compliance. Article seven stipulates that Nextcloud is allowed to keep records of the number of users on the instance to certify its compliance with this agreement, and that the customer is required to keep such records.[70] Nextcloud reserves the right to perform an on site audit if it suspects license abuse by its customer. This means Nextcloud has the legal means to identify the individual end users, and therefore, the collection of the aggregated user data (the number of user statistics) via both the Support App and via the Usage Survey also entails the processing of personal data. In reply to this observation, Nextcloud explained and SURF verified, that admins can disable the Support app and the Usage Survey reports without loss of essential functionality. However, these two functionalities are enabled by default, and result in sharing of (technical configuration) data with Nextcloud, including the user statistics.

According to the Terms and Conditions the governing law is German law, or the law of the country where the Customer has its principal place of business, if such national jurisdiction is a national requirement.[71] SURF by default includes national jurisdiction in Framework Agreements.

The Terms and Conditions include a section about support and incident levels, and response procedures. This section can be qualified as a **service level agreement, or SLA**. The SLA describes different support levels for older versions of the software, depending on the type of license, and how Nextcloud prioritises security issues.

[69] Nextcloud Terms and Conditions, version 3.8, Article 4.
[70] Idem, Article 7.
[71] Idem, Article 11.

Figure 17: Nextcloud SLA security issue definitions

Relevant definitions:

- A critical security issue is when the attacker is able to gain remote code execution on the server as a non-admin user.
- A high security issue is when the attacker is able to gain access to complete user data or any other user.
- A medium security issue is when the attacker is able to gain access to limited disclosure of user data, or when the attacker is able to gain access to a single users' user session, or when the attacker gains access to remote code execution on the server as a non-admin user.
- A regression within version is when functionality that was functional with the initial major release broke in minor or patch releases within the same major version.
- Maintenance covers the Nextcloud server software and all supported apps.

The **amended Data Processing Agreement** between SURF and Nextcloud determines that the DPA prevails over other elements of the agreement.

The amended DPA applies to 4 categories of personal data. The DPA acknowledges that Nextcloud collects limited personal data, and most of the data processing takes place inside of the self-hosted software).

1. Account Data, in two types:
   a. Admin Account Data
   b. Contact Data from procurement officers

2. Diagnostic Data, in three types:
   a. Logs optionally shared by customers with Nextcloud
   b. Logs created by Nextcloud GmbH
3. Support Data (both the contents of support tickets and metadata)
4. Website Data from the restricted access websites, i.e. the admin and support portal.

The amended DPA contains two limitative lists of purposes, authorised processing purposes as data processor – see Section A.5.2.1, and further processing purposes as authorised controller – see Section A.5.2.2.

Nextcloud's standard **Data Processing Agreement** is a template that follows the EC standard contractual clauses for controllers to processors.[72] This template is no longer relevant for this DPIA.

Nextcloud does not apply an **Acceptable Use Policy**, as it does not host any data itself, and hence, cannot impose usage restrictions.

Nextcloud's **Privacy and Legal Policy** covers other processing purposes and includes a section on **Cookies**. The policy applies to processing for which Nextcloud qualifies as

[72] Nextcloud DATA PROCESSING AGREEMENT (DPA) PURSUANT TO ART. 28 (7) GDPR, Commission Implementing Decision (EU) 2021/915 by the European Commission of 04/06/2021, published on 07/06/2021.

independent data controller. Nextcloud writes: "*The aforementioned controller is hereinafter collectively referred to as "the controller" or "Nextcloud" or "we" or "us".*"[73]

The Privacy and Legal Policy applies mostly to the data collection via Nextcloud's public websites, but also includes data processing via reported problems sent to abuse@nextcloud.com and communication with prospective customers, via for example events, social media and the public Nextcloud Forum.

The policy also covers the processing of personal data via the (restricted access) Support Portal, but this is no longer valid for SURF members, as this processing is part of the amended DPA.

The policy describes how data subjects can exercise their rights with Nextcloud as controller, and offers access to a form to submit such a request. Nextcloud provides the contact details of the State Commissioner for Data Protection and Freedom of Information in Baden-Württemberg, but also informs visitors they have the right to file a complaint with their national supervisory authority.[74]

Nextcloud can unilaterally change the content of its Privacy and Legal Policy, without actively informing customers. Though Nextcloud puts a date at the bottom of the policy, it does not offer links to previous versions of its policy, or overviews of changes. In Section XXIII Nextcloud writes: "*We reserve the right to amend this data protection declaration in order to continually adapt it to the applicable provisions, as well as our offerings on our website*."[75] During the drafting of this DPIA, Nextcloud changed a version from August 2025 in a version dated February 2026.

Outside of the enrolment framework with its customers, Nextcloud binds its employees to 4 ethical standards:

- Human Rights Statement[76]
- Code of Conduct[77] (also applicable to developers and users)
- Ethics and Anti-bribery guidelines[78]
- Internal data protection policy[79]

In its Human Rights Statement Nextcloud writes:

"*As a company committed to ethical business practices and upholding fundamental human rights, we align ourselves with the principles outlined in the United Nations Declaration of Human Rights. (...)*

Our commitment to the UN Declaration of Human Rights extends beyond mere compliance with legal obligations. (...)

[73] Nextcloud Privacy and Legal Policy, Section II.
[74] Sections XXI and XXIV.
[75] Section XIII.
[76] Nextcloud, Human Rights Policy, undated, URL: https://nextcloud.com/human-rights-policy/ (last visited 6 February 2026).
[77] Nextcloud, Code of Conduct, undated, URL: https://nextcloud.com/contribute/code-of-conduct/ (last visited 6 February 2026).
[78] Nextcloud, Ethics and Anti-bribery guidelines, undated, URL: https://nextcloud.com/code-of-ethics/ (last visited 6 February 2026).
[79] Not publicly available: Nextcloud share a copy with SURF.

Furthermore, we are dedicated to conducting our business operations with integrity and transparency, ensuring that human rights considerations are integrated into our policies, procedures, and decision-making processes."[80]

The Nextcloud Code of Conduct presents a summary of the shared values and "common sense" thinking in the Nextcloud community. The Code specifies: "*This Code of Conduct is shared by all contributors and users who engage with the Nextcloud team and the Nextcloud-community.*"[81]

Mitigating measures Nextcloud:

- Nextcloud has agreed on an amended DPA with SURF, with an expanded scope and two specific limitative lists of purposes. The new purposes are discussed in Sections A.5.2.1 and A.5.2.2.
- The amended contract with SURF excludes the applicability of the data processing purposes mentioned in Nextcloud's Privacy and Legal Policy for the personal data that Nextcloud can process as a result of the procurement and use of the Nextcloud Enterprise software and services.

A.3 Technical analysis personal data processing

A.3.1 Content Data (only processed by customers)

Because the Nextcloud Enterprise software is self-hosted, only customers themselves have access to the data. There is no logical reason why Nextcloud GmbH would process any Content Data, other than via support and consultancy requests from its customers.

SURF tested if Nextcloud did not perform any checks on the self-hosted software by using a picture of a nipple as avatar and by intercepting all network traffic from the clients and the server. The technical analysis shows that Nextcloud indeed has not programmed the software to communicate any Content Data to itself (no filter, see also point 13 in Section A.4.1).

The Nextcloud Enterprise software includes an open source AI-assistant. SURF tested this functionality for transcriptions of meetings in Talk, and downloaded and installed OpenAI's Whisper Speech-To-Text[82] from the US American repository Hugging Face.

SURF tested with two conversations in English and one conversation in Dutch. A key problem with the transcriptions is the omission of the names of the participants in the transcripts. This makes it difficult to distinguish between the different contributions. Additionally, the transcription in Dutch seems a lot less accurate than the other two transcribed conversations in English, ranging from omissions to misunderstanding of entire passages. See section 4.3 in the Technical Appendix.

[80] Nextcloud, Human Rights Policy.
[81] Nextcloud, Code of Conduct.
[82] Nextcloud, Whisper Speech-To-Text, URL: https://apps.nextcloud.com/apps/stt_whisper (last visited 1 February 2026).

A.3.2 Account Data (admins and commercial contact data)

This DPIA identifies two types of Account Data: data from and about the admins, and Commercial Contact Data, from the persons responsible for the procurement of the Nextcloud licenses.

Admins of the education organisations can manage users, groups and privileges granted to users and groups, and configure the authentication mechanisms. They can use either the Nextcloud (self hosted) admin web interface or use direct ssh access to their (self-managed) server.

Nextcloud admins can provide authentication for end users by integrating with LDAP/Active Directory or SAML-based identity managers like SURFconext. This allows for automated user provisioning and group membership management directly from a central Identity and Access Management (IAM) system. Once connected, both admins and users can synchronise or manually configure profile attributes such as display names and avatars.

None of these data processing activities are visible for Nextcloud GmbH, as they only take place on the self-hosted instance, and are only logged on the self-hosted instance.

Nextcloud GmbH can however process two types of Contact Data: from the admins and from its contact persons, when they contact Nextcloud or subscribe to newsletters. Nextcloud does not (yet) distinguish between the roles. A contact person of Nextcloud is someone who is added (by either Nextcloud GmbH or by another contact person in the institution) to the Nextcloud Enterprise subscription on the support portal.[83] This could be anyone within an institution but is generally the person who is also admin of the self-hosted Nextcloud instance. Currently, Nextcloud automatically sends contact persons both (commercial) customer newsletters and security updates.

In the very limited test setup, the test admin was also the commercial contact person (that procured the licenses), but this is normally not the case for education organisations.

Nextcloud has confirmed that Collabora does not receive contact data from Nextcloud for license registration. Nextcloud only shares the number of licenses and the duration of the contract.[84]

Mitigating measures Nextcloud:

- Nextcloud will offer two types of subscription to Enterprise customers in Q3 2026:
  - Registration as commercial contact for a customer
  - Registration as admin
- In the self-service Nextcloud portal (portal.nextcloud.com) customers will be able to distinguish, when they become customers, if they are admin or commercial contacts. Nextcloud will realise this in Q3 2026.
- The Nextcloud portal will have a functionality for customers to decide themselves to subscribe and unsubscribe to commercial and technical newsletters by the end of Q3 2026.

[83] Nextcloud – Your subscription, URL: https://portal.nextcloud.com/subscription
[84] Nextcloud reply to part A of the DPIA, 2 April 2026.

A.3.3 Diagnostic Data

As mentioned in Section A.2.1, this DPIA distinguishes between three types of Diagnostic Data:

1. Logs only available to customers
2. Logs optionally shared by customers with Nextcloud GmbH
3. Logs created by Nextcloud GmbH

Only the latter two types of Diagnostic Data are accessible for Nextcloud.

Sections A.3.3.1.1 and 0 below discuss the first type, logs stored in the self-hosted Nextcloud software environment, or software managed by a partner as SaaS.

Sections A.3.3.2 (Usage Survey data), 0 (System Information Report) and A.3.3.2.3 (Support App data) discuss the Diagnostic Data admins can optionally share with Nextcloud GmbH, for example as part of a support request.

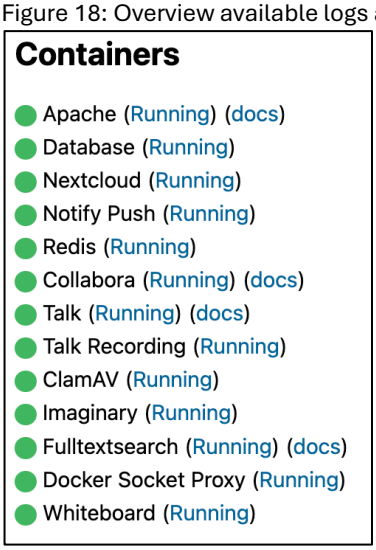
The third type consists of seven other types of logs generated by Nextcloud, discussed in Section A.3.3.3 below.

While the Nextcloud Enterprise software is self-hosted (or managed as SaaS by a third party service provider), and the clients are hosted on the end users' desktops or mobile devices, Nextcloud could have technically programmed the server software and client applications to send metadata about the functioning and use of the software to external domains (including Nextcloud's own domains) but SURF **did not observe such telemetry data traffic** sent to external domains by Nextcloud, neither when interfacing with Nextcloud itself nor when downloading data from external services (like GitHub or Hugging Face).

A.3.3.1 Logs only available to customers

The Nextcloud server software helps admins keep the software secure, up to date and well-functioning by offering access to many different (local) logs that record admin, end user and system activities on the self-hosted server.

Figure 18: Overview available logs applications in the Nextcloud AIO interface on test server



Additionally, Nextcloud offers admins access to 4 additional logs stored in a different location on the Nextcloud server. Admins can easily access these logs via the log reader GUI, provided they have chosen the Nextcloud all in one install option (AIO)

1. Audit logs
2. Interaction logs
3. Installation logs
4. Update logs

Nextcloud explained the core purpose of these logs (which generally should be rotated quickly, 1-2 weeks) is to find issues with the Nextcloud server. The audit log is designed to store user activity for a longer period. The audit log inevitable contains sensitive data on user activity. Nextcloud also stores activity in the Activities app (a separate table in the database, but can also be run on a separate database). This is meant for the users' convenience (see who did what) and has an algorithmic cleanup mechanism and maximum retention period (default 6 months). Activities can be turned off, or retained forever.[85]

SURF enabled and analysed all of the above logs for the processing of personal data, authentication and authorisation data. The contents of the first two logs are discussed in Sections A.3.3.1.1 and 0 below. The latter two logs (installation and update logs) do not contain any personal data, but provide admins with records of installing and updating software versions. The Technical Appendix contains more detailed descriptions and screenshots. As noted in the Technical Appendix, Nextcloud provides documentation about the first two logs (audit and interaction logs) but SURF could not find documentation about the contents of logs of specific apps and containers:

1. Installation logs
2. Update logs
3. Apache logs
4. Database logs

[85] Nextcloud reply to part A of the DPIA, 2 April 2026.

5. Nextcloud Notify Push logs (mobile app push notifications)
6. Redis logs
7. Collabora Online logs
8. Talk interaction logs (see Section 0 below)
9. Talk recording logs
10. ClamAV (local antivirus) logs
11. Imaginary (for displaying images) logs
12. Fulltextsearch (faster search, indexing) logs
13. Docker Socket Proxy logs (backbone for AppAPI)
14. Whiteboard logs

None of these logs are accessible for Nextcloud GmbH. SURF could not find documentation from Nextcloud describing all available logs. When SURF inquired Nextcloud about this, the company was not able to provide such a list, but referred to the log documentation SURF had already accessed.

Nextcloud also provides a server info app to admins for system monitoring. The system monitoring allows administrators to track hardware performance, application metrics, and metrics of active users (see Section 5.3 in the Technical Appendix). Again, Nextcloud GmbH does not have any access to these data.

A.3.3.1.1 Audit logs

The audit logs contain technical metadata like a unique request ID, userID, the app (which part of Nextcloud was used), a description of what happened (like "*Login successful*"), the event severity level, a timestamp, and the software version. For this DPIA 3 types of audit logs were relevant:

1. Login attempts
2. File access by users
3. Automatic deletion tasks

The contents of these audit logs are described below. Nextcloud publishes a complete list of its logs and contents.[86] On the restricted access page for admins about audit logs, Nextcloud provides a breakdown of types of activities that are logged, but does not explain if the log can contain sensitive or identifying information. See Figure 20 below.

[86] Nextcloud, Logging, page undated, URL: https://docs.nextcloud.com/server/latest/admin_manual/configuration_server/logging_configuration.html (last visited 18 May 2026).

Figure 19: Nextcloud documentation of contents of audit logs[87]

Log field breakdown

- **reqId** (request id): any log lines related to a single request have the same value
- **level**: logged incident's level, always 1 in audit.log
- **time**: date and time (format and timezone can be configured in config.php)
- **remoteAddr**: the IP address of the user (if applicable – empty for occ commands)
- **user**: acting user's id (if applicable)
- **app**: affected app (always admin_audit in audit.log)
- **method**: HTTP method, for example GET, POST, PROPFIND, etc. – empty on occ calls
- **url**: request path (if applicable – empty on occ calls)
- **message**: event information message
- **userAgent**: user agent (if applicable – empty on occ calls)
- **exception**: Full exception with trace (if applicable)
- **data** additional structured data (if applicable)
- **version**: Nextcloud version at the time of request

Empty value are written as two dashes: `--`.

Figure 20: Nextcloud overview of logged activities in audit logs[88]

Logged events

Files

- File
  - created
  - accessed
  - updated
  - renamed
  - copied
  - removed
  - deleted
- File version
  - restored
  - deleted
- File shared with/unshared from (including set permissions and expiration date)
  - user
  - group
  - public link
  - email recipient
  - Talk conversation
  - Circle
  - remote user (federation)
  - remote group
- Share permissions changed
- Password of public share changed

[87] Idem.

[88] Using the audit log – Nextcloud Portal, URL: https://portal.nextcloud.com/article/Compliance/Using-the-audit-log

- Expiration date changed
- Public share having been accessed
- Trashbin
    - file deleted from trashbin
    - file restored from trashbin
- Image preview accessed

Authentication

- Login successful/failed
- Two Factor login attempt successful/failed
- Logout

User management

- User created/deleted
- User enabled/disabled
- Email address changed
- Password changed
- UserID assigned/unassigned
- Group created/deleted
- User added to/removed from group

Apps management

- App enabled/disabled
- App limited to user groups

The audit logs track successful and unsuccessful **login attempts**, with the specific username and authentication method. For requests originating externally (i.e. visits from the end users to the software hosted by SURF on its own server), the logs also document the remote IP address and the User-Agent string. The user agent string provides details about the browser or client software used to access the system.

The read access logs record whenever a file is accessed, for all files, with the specific file ID and the full directory path to the resource, including who accessed this resource. This helps admins see who did what and when. This type of logging is necessary for institutions to be able to track the scope and impact of incidents with unauthorised access. The sample log includes the names of accessed files. Such names can contain personal data such as the name of the person who wrote or redacted a file. Nextcloud does not offer access via its Nextcloud Hub web interface, only via SSH on the server (or via the running link next to a container). This inherently limits unintentional access. Organisations that are concerned about unnecessary access by their admins can also limit the access to the audit logs to for example the root admin.

The audit logs also record automated background tasks. For this DPIA the logs of **deletion operations** are relevant. The Technical Appendix describes 4 examples of automated deletion logs: in Calendar for outdated participation, in Talk for deleted inactive meeting rooms, in Trashbin for files that are stored beyond a predefined lifetime, and in Files for outdated earlier versions. The first two types of logs do not contain any Content Data, such as names of meetings or meeting rooms, but the latter two logs do include the names of files and users.

Nextcloud does not change its audit logs. If an organisation has to systematically delete personal data in Content Data after a certain period, or manually, because it doesn't have a legal ground for the processing anymore, the deleted personal data are still part of the Content Data in the titles or meeting names in the (local) audit log. For example, a CV from a job applicant that is not hired, should be removed within 4 weeks. Commonly, such CVs are stored with the name of the applicant in the title of the document. Even if the organisation deletes that file, the name of the job applicant is still part of the audit log, as part of the name of the deleted file.

This is intentional behaviour, Nextcloud explained, as it considers the audit log the single immutable source of truth. SURF asked Nextcloud if it would be willing to help customers comply with deletion obligations, by offering options to mask deleted Content Data such as file names in the audit log (without deletion of the record of the action, be it deletion or another other action). Nextcloud explained such deletion of information from the audit log does not strike the right balance between stability, security, privacy and maintainability. According to Nextcloud customers can take such privacy protection measures themselves, as they should export the logs generated by the software to professional log management tools. Nextcloud wrote: "*Especially the audit log should be stored in specifically designed software for that purpose which does not allow modification of the logs (write once read many) and can have privacy-protecting features. This is also typically the case for especially larger customers like SURF.*" [89]

Mitigating measures Nextcloud:

- Nextcloud has committed to offer customers an extra export option of the immutable audit logs by the end of 2026, export of the logs with personal data such as meeting and file names masked with ****REMOVED SENSITIVE VALUE**** for customers to import in their own log management tools.
- Nextcloud has also committed to provide more detailed information about the existence of the different logs for admins and better explain when Nextcloud logs can record sensitive and identifying information in the audit logs, in Q3 2026.

A.3.3.1.2 Talk interaction logs

Every time a user connects to a Talk room, Nextcloud Talk logs the specific username, the backend host, the remote IP address, the country this IP address originates from and a detailed User-Agent string identifying the browser and operating system in interaction logs. The Talk logs also track when users join or leave specific rooms by recording the room ID and a unique room session ID. These logs are discussed separately in this DPIA because Nextcloud doesn't make these logs available in the same way as the Nextcloud Office Hub and Files audit logs.

The interaction logs include the user name, but do not include the room name. Only when hosts remove room sessions or if the rooms are automatically removed after a predefined expiry time, the logs do show the names of rooms, such as in the SURF test scenario, the name "euthanasie en abortie".

[89] Idem.

To prevent unnecessary access by admins to identifiable user names or removed room names (and to limit the impact of potential data breaches), SURF has asked Nextcloud to help admins by offering a specific export option of the interaction logs in which the names of users and names of removed rooms in the logs are automatically masked by ****, with an option to retrieve the specific names from the raw interaction logs if necessary. Nextcloud has agreed to implement this measure by the end of 2026.

There are also data processing activities that Talk does not log. This is the case for events related to recording of meetings: there are no logs about starting and stopping of a recording, or logs of activities in Whiteboard and user poll (nor the setup, nor the voting). Nextcloud does not log interactions in the chat, like sending chat messages and reacting to messages with emoji. The absence of 'memory' about these data processing activities is a good example of data minimisation: this helps organisations prevent abuse of the logs as employee monitoring system.

Nextcloud explained in reply to this DPIA that Nextcloud should and will expand the audit logs over time to provide an adequate resource for legal reasons and for security related actions, but Nextcloud will not start recording contents of data inside chats or documents or polls.

Nextcloud provided the following list of examples of actions that are relevant for audit logs:

- *Who accessed what data and when.*
- *When did someone share or download a file, or modify it.*
- *When was somebody added or removed to a deck board.*
- *When did somebody gain access to a Table or lose it again.*
- *When did somebody join or leave a Talk room (and thus have access to messages therein) etc.*
- *When did somebody enable/disable 2-factor authentication, or log in and log out.*
- *When did they enter a password and from where (most of the time, ppl stay logged in - so this should catch a login from, say, a internet cafe in a unknown place).*
- *When did who add a security policy, or modify an existing one, or apply it to a set of data.*

Participation in polls is not relevant for the audit logs, and is (and will) therefore not (be) recorded. Even though the poll results itself do not include names or IP addresses of the participants, in the tested case the poll was not 'anonymous' as Nextcloud currently writes, but pseudonymous, because the host in the test scenario could see the result from a single other known participant. As explained in Section A.2.2.1 above, re-identifiability is reasonably possible with 3 participants, and if the poll refers to a document, even with more participants.

Mitigating measures Nextcloud:

- Nextcloud has committed to offer customers an extra export option of the Talk logswith personal data such as user and meeting names masked by ****REMOVED SENSITIVE VALUE**** for customers to import in their own log management tools, by the end of 2026.

- Nextcloud will replace the current explanation that the polls are anonymous' by: "*(re)identification of poll participants is highly unlikely*" in Q3 2026.
- Nextcloud will provide a better explanation to admins about the possibly sensitive contents of the Talk interaction logs, and what the Talk logs intentionally do not register, in Q3 2026.

A.3.3.2 Logs that admins can optionally share with Nextcloud

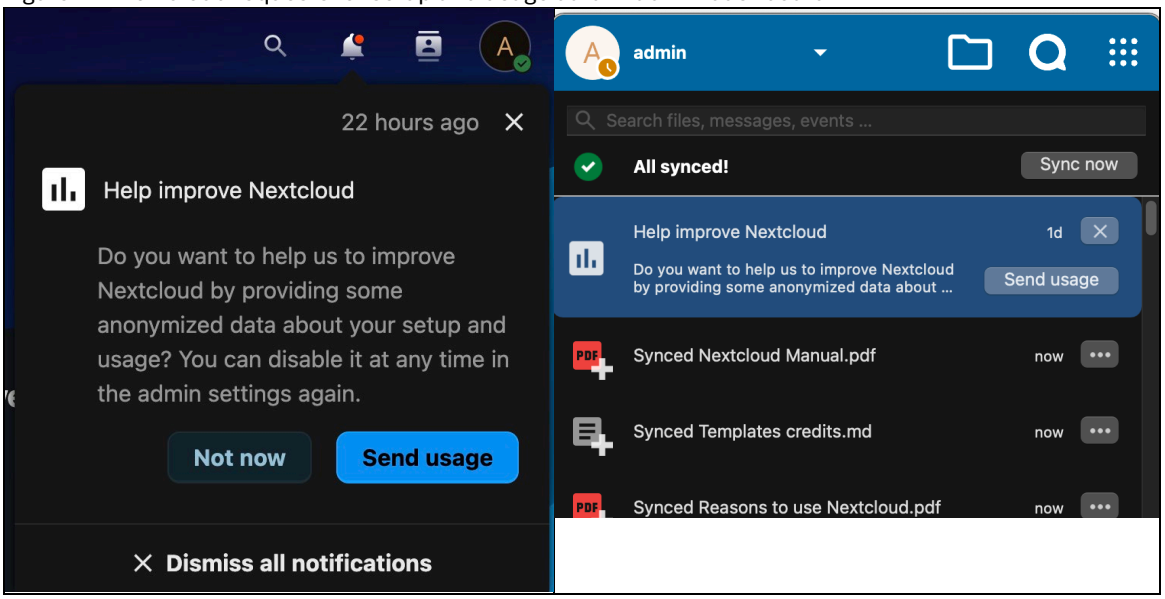
Admins can share Diagnostic Data with Nextcloud in three ways: by sharing Usage Survey Data, by creating a System Information Report and sharing a link with Nextcloud, and finally, automatically, by using the Support App.

A.3.3.2.1 Usage Survey Data

Nextcloud includes an option called 'Usage Survey'. Upon a new install of Nextcloud, the admin was prompted to participate in the Usage Survey. This functionality is only available to admins. If admins consent, they will share server data with Nextcloud. Nextcloud emphasises the data are '*anonymized*'. See Figure 21 below.

In reply to a question from SURF, Nextcloud changed the wording of the 'Not now' button to 'No', and wrote it disabled the monthly reminder questions to admins to share the Usage Survey.[90]

Figure 21: Nextcloud requests for setup and usage data in admin dashboard[91]



In its Privacy and Legal Policy Nextcloud describes it immediately aggregates the Usage Survey Data after collection:

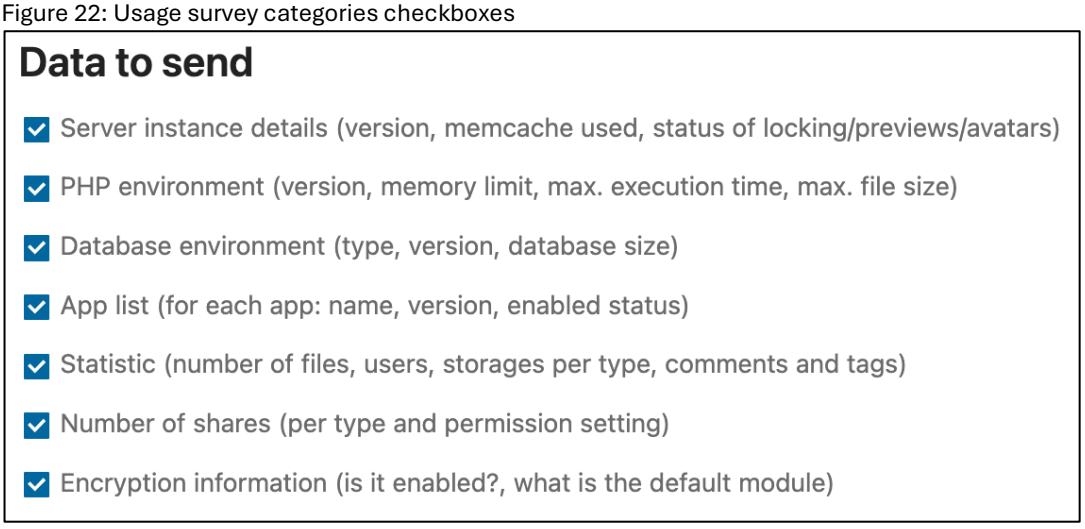
"The optional Usage Survey app (usage report) can send us statistical data about the use of the instance, such as installed apps. This data helps us improve our services. You have the

[90] Nextcloud reply to part A of this DPIA, 2 April 2026.
[91] Screenshots taken 6 November and 4 December 2025 in the SURF test instance

option of checking and authorising this data before it is transmitted. We store the data in an aggregated form and not on a single server basis. As a result, this data cannot be used to draw conclusions about the information of an individual instance in the event of a data leak [underlining added by SURF]."[92]

If an admin agrees, the server will automatically share a monthly report with Nextcloud. Admins can untick categories of data, or choose manual sending instead of monthly.

Figure 22: Usage survey categories checkboxes



As shown in the Technical Appendix, Nextcloud collects the unique ID of the Nextcloud instance (in the test case: ocee3ii9ih59) in the Usage Survey data. This means Nextcloud is technically capable of linking the dataset over time to a specific Nextcloud instance. Since Nextcloud automatically collects the IP address of the server (separately from the contents of the Usage Survey Data), and the server is connected to a DNS record (with registration of the domain name administrative contact), Nextcloud has access to identifying data from the customer. It also follows from Nextcloud's reply to the DSAR that it was able to connect the requesting admin to this server ID, and reproduce the filed Usage Survey data. Since Nextcloud collects statistics relating to users that are identifiable for the customer, this data collection should be qualified as pseudonymous personal data even if Nextcloud uses the Usage Survey data in aggregated form.

In reply to this observation, Nextcloud explained it logs limited information about the current Nextcloud version used by the customer to provide the right updates, as well as logs about downloads, and automatically collects the IP address of the customer tenant. Nextcloud initially did not explain why it collects the customer instance ID with the Usage Survey.[93] Nextcloud also didn't explain how it aggregates the Usage Survey data, how long it retains the identifiable identifiers.

[92] Nextcloud, Privacy and Legal Policy, August 2025, URL: https://nextcloud.com/privacy/
[93] Nextcloud reply to part A of this DPIA, 2 April 2026.

Mitigating measures Nextcloud:

- Nextcloud changed the wording of the choice to share the Usage Survey from Yes/'Not now' button to Yes/'No', and has disabled the monthly reminder questions to admins to share the Usage Survey.[94]
- Nextcloud has explained that it retains the Usage Survey Data with the unique instance ID for 1 year.

A.3.3.2.2 System Information Report

As described in more detail in Section 6.3 of the Tech Appendix, admins can install the Nextcloud Support App. This offers a web interface for admins to create a System Information Report, to view the subscription key and to look up the contact information from the account manager.

If an admin generates a System Information Report the support app generates a password protected public link, which the admin can share with Nextcloud support. The link is valid for two weeks.

The generated System Information Report contains information about versions of the software and configurations. The report generally doesn't contain information that can reveal privacy/security sensitive or confidential information, with one exception relating to Talk.

Nextcloud has taken steps to remove identifying data from the report, as marked by Nextcloud with the words: "****REMOVED SENSITIVE VALUE****". This prevents Nextcloud from collecting the ID of the Nextcloud instance, or passwords/secrets/tokens and hostnames. However, the report does include some data that can help identify the specific customer, such as "svcnextcloud.duckdns.org" and https://svcnextcloud.duckdns.org/standalone-signaling/. These are URIs to SURF's Nextcloud environment used for this DPIA. Nextcloud is capable of identifying its customer SVC (SURF Vendor Compliance) from the URI, and has identifying contact data of the admin and commercial contact persons.

In reply to this observation, Nextcloud explained: "*The host names are relevant for Talk related issues and it is important for the Talk team to have this data. We need to know if the domains in both fields are the same and if the protocols are correct (wss instead of http). Not having this data increases the risk of overseeing what caused the issue, and in case there are problems related to STUN/TURN we need to have the data anyway to ping those locally and test.*"[95]

A.3.3.2.3 Diagnostic Data via Support app

Nextcloud explained that the Support app periodically sends Diagnostic Data to Nextcloud, separate from the option for admins to create a System Information Report: "*The Support app periodically sends us some information about the server, including the number of users. This app can be disabled and our contract does not require it to be enabled. If it is*

[94] Nextcloud reply to part A of this DPIA, 2 April 2026.
[95] Nextcloud reply to part A of the DPIA, 2 April 2026.

disabled, we reserve the right to conduct an audit of the customers' records in case there are reasons to suspect the customer is breaching the license agreement by having more users than paid for.

Information we receive:
subscription key
instance id
user count
version
active user count
app list"[96]

Nextcloud additionally explained:

"The Support app itself does not collect or store IP addresses. For subscription validation, the customer's Nextcloud instance establishes a connection to our subscription endpoint. The source IP address (the server IP of the instance, not end-user IPs) is technically visible to the receiving server. These logs are stored seven days."[97]

SURF did not observe this periodical traffic during the limited testing.

Mitigating measure Nextcloud:

- Nextcloud will publicly document the data sharing via the Support app in Q3 2026.

A.3.3.3 Logs generated by Nextcloud GmbH

Nextcloud can remotely create seven types of logs with personal data that are not accessible for admins:

1. Software download and update log
2. Push notification proxy log
3. Activity log in Zammad's support ticketing system
4. Webserver access log (visits to the restricted access Support Hub website, to portal.nextcloud.com, and Nextcloud's publicly accessible nextcloud.com website)
5. Log of outbound email to customers including newsletters (via ActiveCampaign / Postmark)
6. License distribution log (via Sendent, only in this specific test scenario[98])
7. Log of privacy / access requests (via DataCo)

Processing via these logs, including via (sub-)processors, is relevant for this DPIA, because the processing is indispensable for the integrity, availability, and compliance of the

[96] Nextcloud reply to part A of the DPIA, 2 April 2026.
[97] Explanation Nextcloud in correspondence about DPA, 2 July 2026.
[98] In reply to questions from SURF about the data processing by Sendent, Nextcloud explained: "*This is not a default. Sendent develops optional components that can be bought on request. If you purchase Nextcloud Enterprise in the Ultimate plan, their products are included and therefore will be provided in addition to our license*." Reply Nextcloud 6 May 2026. To provide SURF with a single Enterprise test license, Nextcloud also used Sendent.

Enterprise environment, even though the Nextcloud Enterprise is intentionally designed to process all data locally, only accessible for the customer.

For instance, the log about installed software updates, the verification of licenses via Sendent, the processing of support tickets via Zammad and the processing of privacy requests via DataCo constitute processing activities that are an inseparable part of the functionality of the Nextcloud Enterprise software. If these external channels (managed or commissioned by Nextcloud GmbH) process personal data (such as admin metadata, IP addresses, or communication logs), and the education organisation does not have any contractual control over the purposes of the data processing by these external end points, it has to consider these organisations as third parties, and assess the legal ground for disclosure of personal data to these third parties.

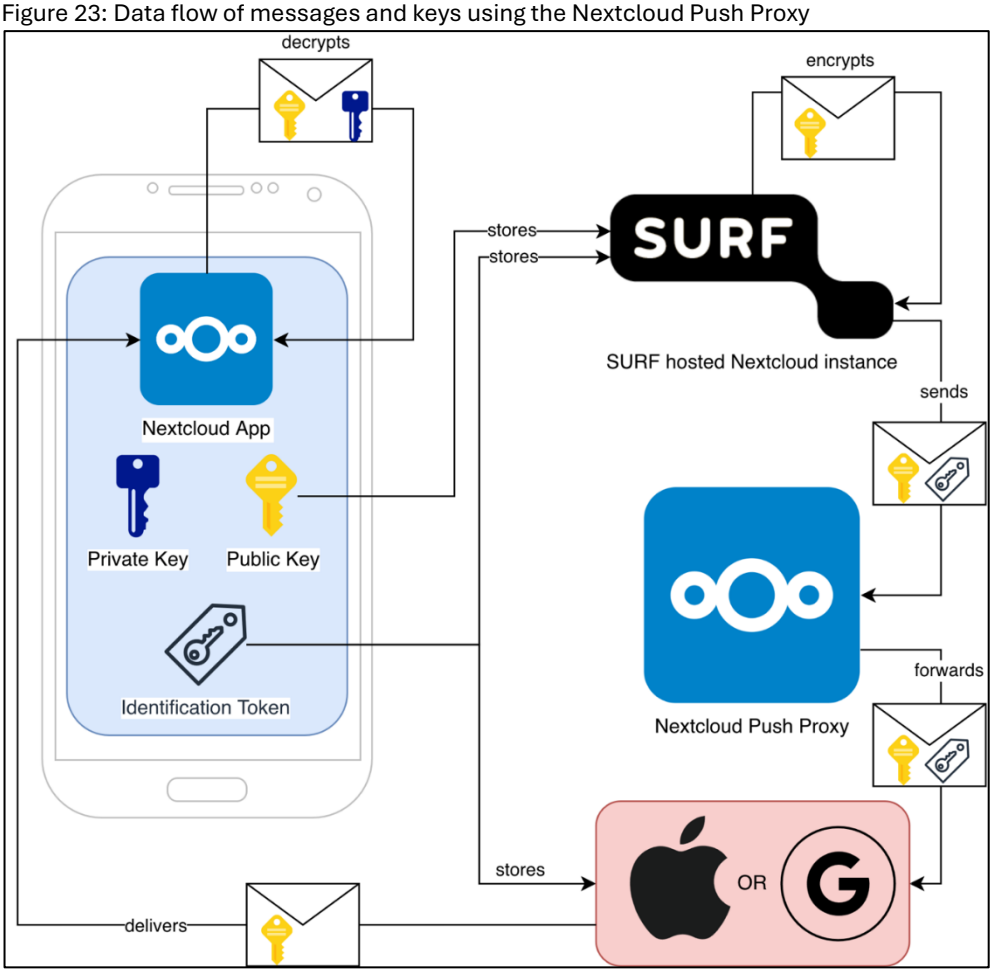
As explained in the Technical Appendix (Section 6.4.2), Nextcloud keeps a log of (server) **software updates**. Whenever an admin downloads a new version of the software from Nextcloud's hosted repository (not from its GitHub repository), the download request is logged. The logs include the Subscription ID and configuration information. The data are purged after 14 days.

Nextcloud explained it only stores two data points from the **push notification proxy** logs: "*We process the date on which the device was registered as well as the public key used for push notification delivery.*"[99] Nextcloud also explained: "*When you log into one of our mobile apps, a public and private key are generated on the device itself, and the public key is sent to your Nextcloud @instance. When a push notification is sent to your device, that public key is used to encrypt the data before sending it to the Nextcloud Push Proxy. Only after receiving the notification on the device is it decrypted using the private key of the device.*
The push proxy passes on encrypted notifications, it cannot read what's inside them.
The proxy needs to remember which device belongs to which user, so it knows where to forward notifications when they arrive. Without that stored mapping, it would have no way to deliver the message to the right device."[100]

SURF visualised the data flow of messages and keys in Figure 23 below. The data processing via Google and Apple is out of scope of this DPIA.

[99] Nextcloud answers to SURF questions, 9 February 2026.
[100] Nextcloud reply to part A of the DPIA, 2 April 2026, in reply to a question about the retention period of these logs.

Figure 23: Data flow of messages and keys using the Nextcloud Push Proxy



The Support Portal is hosted by an external party (Zammad). Zammad creates a separate **access log** to record what actually happened on the system, meaning technical events such as access and system activity.

Nextcloud has explained to SURF the Zammad Production Log contains the following data:

- User actions (ticket creation, updates, login events)
- Internal application processes
- Errors and warnings
- API requests
- Database interactions
- Permission problems
- Email processing results
- Incoming mail fetch results
- IMAP/POP3 connection status
- Mail parsing errors
- Ticket creation from emails
- Successful logins
- Failed login attempts
- Session creation

- Logout events
- API authentication
- OAuth / LDAP authentication (if used)

Zammad retains these logs for 42 days.[101]

For security and data protection reasons Zammad does not provide Nextcloud or other customers with direct access to these log files, but can provide access to relevant log data when legitimately required, for example in the context of:

- Security audits
- Incident investigations
- GDPR-related requests or other legally justified inquiries. [102]

Nextcloud also wrote: "*The majority of personal data relevant to the data subject is already accessible through the user interface. Nextcloud commits to provide access request in accordance with GDPR obligations if customers cannot access specific information via the UI.*"[103] See the box with mitigating measures at the end of Section A.3.6.1.

Nextcloud explained it deletes the **webserver access logs** within seven days. Based on the logging schema Nextcloud logs very little data.

Figure 24: Contents of webserver access logs

127.0.0.1 - frank [10/Oct/2000:13:55:36 -0700] "GET /apache_pb.gif HTTP/1.0" 200 2326 "http://www.example.com/start.html" "Mozilla/4.08 [en] (Win98; I ;Nav)

Next to its own webserver access logs Nextcloud also enables to third parties to collect Website Data**: GitHub and Hugging Face**. While Nextcloud Hub releases are available via portal.nextcloud.com, Nextcloud refers customers and end users to GitHub and Hugging Face to download specific software components, including AI models and various Nextcloud Apps. Notably, the Nextcloud All in One package is exclusively sourced from GitHub for its initial setup. This remains the official installation method prescribed by Nextcloud, as outlined in Nextcloud's own technical documentation.[104]

Nextcloud uses the US American **mail delivery provider ActiveCampaign** (owner of the service called Postmark since 2024) to send its newsletters. Nextcloud informed SURF that the Postmark logs contain Message ID, Status (Delivered, Processed, Undeliverable), Email address, Subject, Tag (always empty), Date and Time, Bounce reason (if undelivered). [105]

Additionally, Nextcloud logged 'engagement' with the mails, such as 'opened' and 'clicked'.by including a tracking pixel in the mails made with the open source software Odoo. In reply to this DPIA, Nextcloud has disabled the tracking pixel. See Section A.10.

[101] Nextcloud reply to part A of the DPIA, 2 April 2026.
[102] Idem.
[103] Ibid.
[104] Nextcloud, How to install the Nextcloud All-in-one on Linux, URL: https://nextcloud.com/blog/how-to-install-the-nextcloud-all-in-one-on-linux/
[105] Nextcloud reply 6 May 2026 to questions SURF 17 April 2026.

Nextcloud did not provide information about the data processing to **distribute licenses**, in this case by Sendent. According to Nextcloud Sendent was only incidentally involved for the specific set-up for SURF, not systematically. See the explanation in Table 4.

With regard to **privacy requests** filed via the DSAR form as managed by DataCo, Nextcloud explained DataCo was a subprocessor. Nextcloud has also engaged DataCo as external privacy officer, in that case, as independent controller (out of scope of this DPIA).

Mitigating measure Nextcloud:

- Nextcloud is actively searching for an EU-based provider of mail services, and expects to switch in Q3 2026.
- Nextcloud has disabled the tracking pixel in its commercial and security newsletters.
- Nextcloud will publicly document the limited logs the company collects, and their retention periods, in July 2026. SURF has reviewed and approved of this documentation.
- Nextcloud has clarified the different retention periods of these logs – See Section A.11.2.

A.3.4 Support Data

Nextcloud only provides third level support: the education organisation itself must provide first and second level user support.[106]

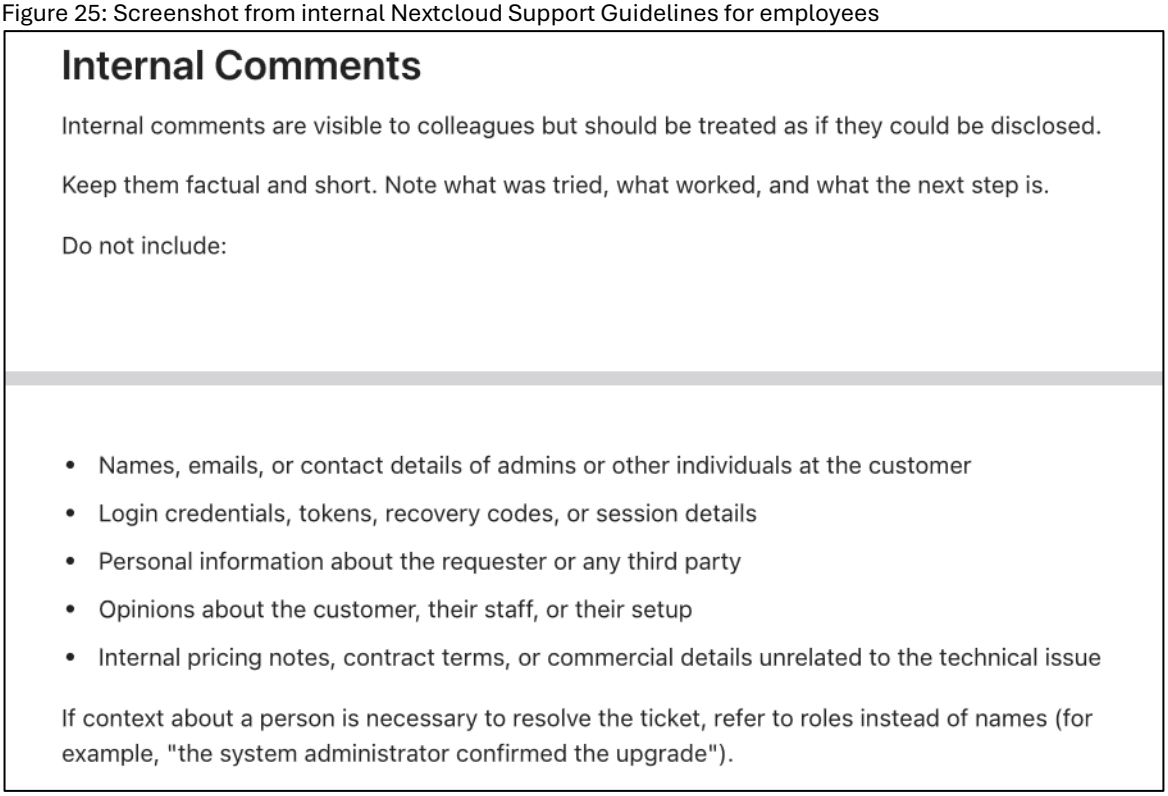
Nextcloud provides support via an external support portal, from (sub-processor) Zammad. Nextcloud explained it does not have direct access to the metadata about support tickets. Zammad only provides session data from the Support Hub to Nextcloud, nothing else, no historical logs. Nextcloud also explained only two people at Zammad have access to these logs.[107]

Customers cannot export the support tickets or delete them. They can file a request with Nextcloud to delete some or all tickets prior to the agreed default retention period of 15 months for all SURF members.[108] See Section A.11.2 for an explanation about this agreed retention period.

In reply to a question from SURF, Nextcloud showed the interface of the Zammad Portal for Nextcloud (and Collabora) support employees. The interface includes an open text field for employees to enter comments, but Nextcloud also shared the instructions in its Support Guidelines for employees to not include any personal data or opinions about the customer.

[106] Nextcloud Enterprise Terms and Conditions, v3.8m, Recital e).
[107] Nextcloud answer to SURF questions, 9 February 2026.
[108] Nextcloud answer 6 May 2026 to SURF questions 17 April 2026.

Figure 25: Screenshot from internal Nextcloud Support Guidelines for employees



Internal Comments

Internal comments are visible to colleagues but should be treated as if they could be disclosed.

Keep them factual and short. Note what was tried, what worked, and what the next step is.

Do not include:

- Names, emails, or contact details of admins or other individuals at the customer
- Login credentials, tokens, recovery codes, or session details
- Personal information about the requester or any third party
- Opinions about the customer, their staff, or their setup
- Internal pricing notes, contract terms, or commercial details unrelated to the technical issue

If context about a person is necessary to resolve the ticket, refer to roles instead of names (for example, "the system administrator confirmed the upgrade").

The Support Data include the ticket metadata as integral part of the ticket itself.

These metadata include the ticket ID and number, title, status, priority, assigned group and owner, customer and organization references, timestamps (creation, last update, last contact, response and close times), tags, and any custom fields configured in the system. If a support ticket is deleted, these metadata are also automatically deleted.

Zammad also maintains a separate activity log. The contents of this log are discussed above, in Section A.3.3.3.

SURF generated 5 support tickets with Nextcloud via the Zammad support portal (support.nextcloud.com). These tickets were sometimes generated by default such as “Nextcloud Outlook Add-In” and “Nextcloud Talk High Performance Backend”, but SURF also actively submitted a request regarding the inability to add colleagues to the subscription.

According to its Enterprise Terms and Conditions, only Nextcloud GmbH located in Stuttgart Germany provides support, but this only applies to 3 of the 4 tested core applications Files, Groupware and Talk. The test set-up included Nextcloud Office, supported by Collabora Online from the UK. Nextcloud explained that employees working for Collabora can access the relevant support tickets in Zammad (but not any other tickets or customer information).

Admins with an Enterprise license can access the support portal. The portal shows an overview of tickets. In the SURF test instance, Nextcloud showed 5 communications, even

though SURF had only filed 1 ticket. The other 4 tickets were messages from Nextcloud about the support options.

Admins cannot delete tickets or attachments themselves. Nextcloud initially did not show a warning to admins not to upload sensitive personal data when they upload attachments, but immediately added this upon receipt of part A of this DPIA to the portal page where new tickets can be submitted. See Figure 27. However, Nextcloud did not (yet) add this warning to the formal support page, where admins can view and respond to existing tickets. See Figure 28 below.

Figure 26: Nextcloud support portal with 5 tickets

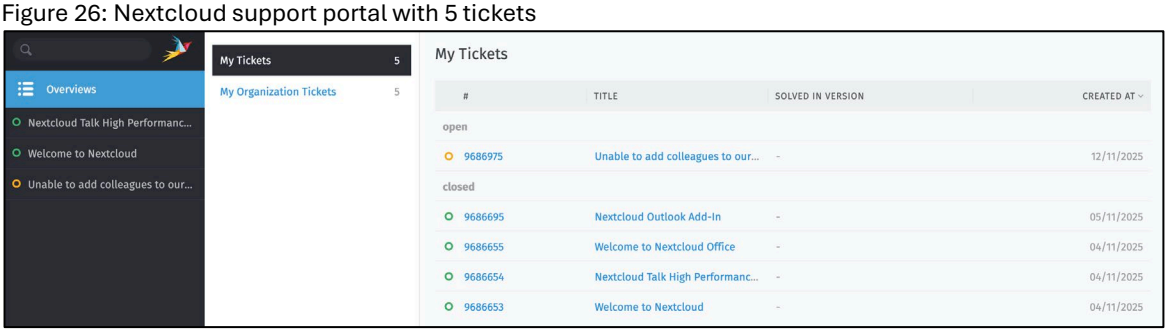


Figure 27: New warning in 'Submit a ticket' on portal.nextcloud.com to admins

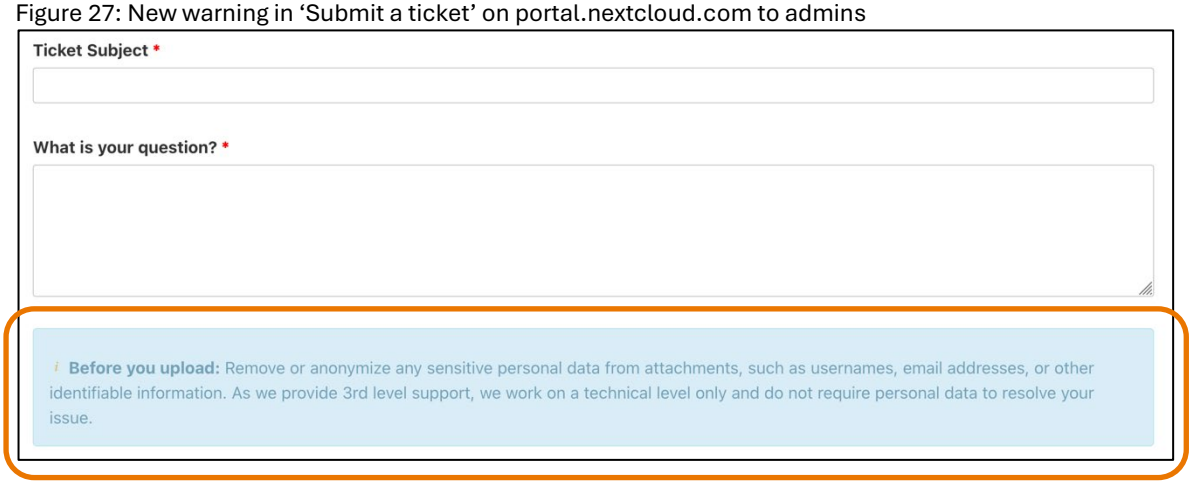
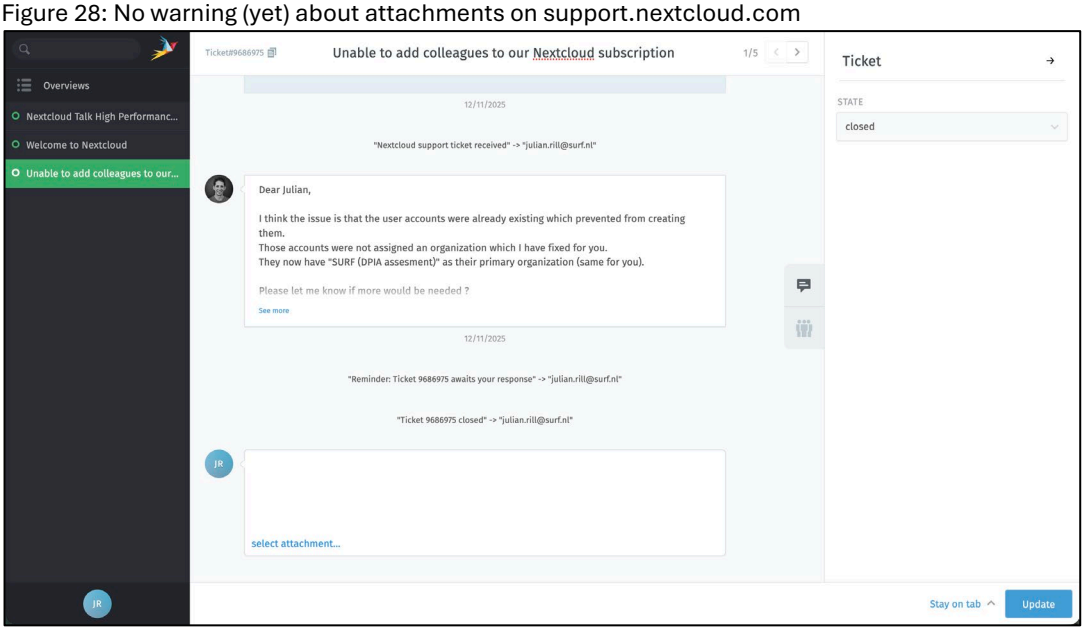


Figure 28: No warning (yet) about attachments on support.nextcloud.com



Mitigating measures Nextcloud:

- Nextcloud has added a warning for admins on portal.nextcloud.com not to upload any personal data in attachments.
- Nextcloud has agreed with Zammad to implement the same warning on support.nextcloud.com in Q3 2026.
- Since 10 May 2026, only Collabora employees physically located in the UK and the EU can access the relevant tickets in Zammad, not any employees located in other countries outside of the EU.
- In case the adequacy decision for the UK is no longer valid, Nextcloud will ensure that only EU based employees of Collabora can access the support tickets.
- Nextcloud and SURF have agreed on a default retention period for the support tickets of 15 months (instead of the default 4 years). Customers can ask Nextcloud to remove specific or all support tickets and attachments before a certain date.

A.3.5 Website Data (including cookies)

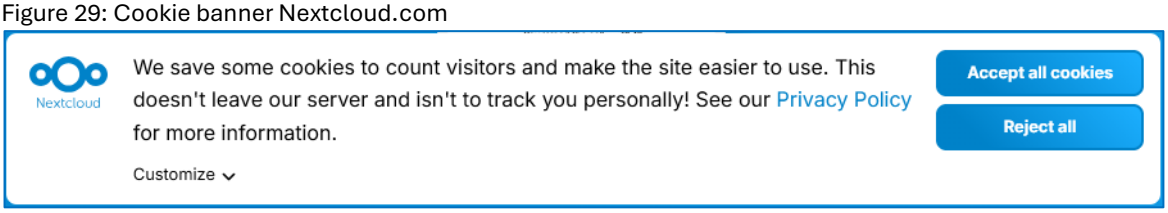
SURF has analysed the data processing via 3 different relevant sources: Nextcloud's two types of relevant websites and cookies set by the self-hosted server software.

1. Legal and technical documentation at public website nextcloud.com (https://nextcloud.com/privacy/ and https://docs.nextcloud.com/server/latest/admin_manual/)
2. Restricted access Support Portal, via nextcloud.com/support/ (including portal.nextcloud.com/)
3. Self-hosted Nextcloud server software.

A.3.5.1 Cookies at nextcloud.com

On its publicly accessible website, Nextcloud uses a cookie banner.

Figure 29: Cookie banner Nextcloud.com



If a user selects 'Customize', Nextcloud shows four cookie categories (Essentials, Convenience, Statistics and External Media), with details of the cookies set in these categories (name, description, expiry and whether the user has given consent per cookie). See Figure 30 below.

SURF initially did not accept any cookies (did not choose between accept or reject) and did not observe any analytical or tracking cookies. Nextcloud only set the cookie 'wp-wpml_current_language, part of the cookie category 'Essentials' (as shown in Figure 30 below).

In contradiction with the public cookie documentation Nextcloud set two non-essential cookies after SURF rejected all cookies. Nextcloud set the two convenience cookies 'nc_form_fields' and 'nc_utm_parameters' on SURF's end device, without the consent Nextcloud states it asks. When SURF retested on 16 April 2026 both cookies were empty, but this doesn't prevent collection of some data such as the visitor IP address.

SURF did not observe setting of cookies when visiting Nextcloud's documentation subdomain www.docs.nextcloud.com.

Figure 30: Nextcloud detailed cookie explanation on nextcloud.com

Table 2: Cookies found in traffic to Nextcloud public website without consent

Host	Cookie	Referrer	Note
nextcloud.com	wp-wpml_current_language	nextcloud.com	Essential session cookie
nextcloud.com	nc_utm_parameters	nextcloud.com	Convenience session cookie

nextcloud.com	nc_form_fields	nextcloud.com	Convenience session cookie
nextcloud.com	nc_cookie_banner	nextcloud.com	Essential session cookie

Mitigating measures Nextcloud:

- Since 29 April 2026 Nextcloud no longer by default sets the two observed convenience cookies (at all, not empty either).

A.3.5.2 Cookies set by Support Portal

Nextcloud provides two additional web pages for Enterprise users to allow users to manage their subscription and submit support tickets. Both these pages operate under the same user identity, i.e. a user with an account can login to both support.nextcloud.com and portal.nextcloud.com with the same username and password.

SURF did not observe a cookie banner on either website, or any description of the cookies. SURF did however not observe any analytical or tracking cookies. SURF observed that there is no persistent cookie for keeping login data. This means a user needs to relog in upon session end.

There was an issue with missing and vulnerable 2 Factor Authentication, which will be solved in the summer of 2026. See Section A.6.1.3, also for the mitigating measure.

Table 3: Cookies found in traffic to restricted access Support Portal

Host	Cookie	Referrer	Note
support.nextcloud.com	_zammad_session_b8c1978f060	support.nextcloud.com	Session cookie
portal.nextcloud.com	PHPSESSID	portal.nextcloud.com	Session cookie

Mitigating measures requested from Nextcloud:

- Nextcloud will publish accurate information about the (first party) functional cookies it sets on its admin and support Portal in July 2026.

A.3.5.3 Cookies set by self-hosted server

Nextcloud does not show a cookie banner to the end user during the usage of the (self-hosted) Nextcloud environment. This implies that all cookies that are set or read should be functional, strictly necessary cookies (no consent required). Nextcloud confirms on a technical support page it only sets 3 first party cookies.[109]

[109] Nextcloud GDPR compliance, Cookies, page undated, URL: https://docs.nextcloud.com/server/latest/admin_manual/gdpr/cookies.html#cookies-stored-by-nextcloud (last visited 6 February 2026).

The analysis of the intercepted data traffic shows that Nextcloud has not programmed the server software to use third party cookies. The customer (SURF in this case) collects some first party session cookies.

As shown in Table 6 in the Technical Appendix, one of the cookies included the pseudonymous unique identifier of the test instance. The purpose of this data processing was unknown, as the cookie was not mentioned in Nextcloud's documentation.

Mitigating measures Nextcloud:

- Nextcloud has updated its cookie documentation for the self-hosted software. Nextcloud now explains the instance ID is "*used to identify the user on the server.*"[110]
- The updated cookie information now includes 3 previously missing types of information:
  - The exact names of the cookies the software sets.
  - The purposes of the cookies, with sufficient granularity.
  - The expiry date of the cookies.

A.3.6 Results Data Subject Access Request

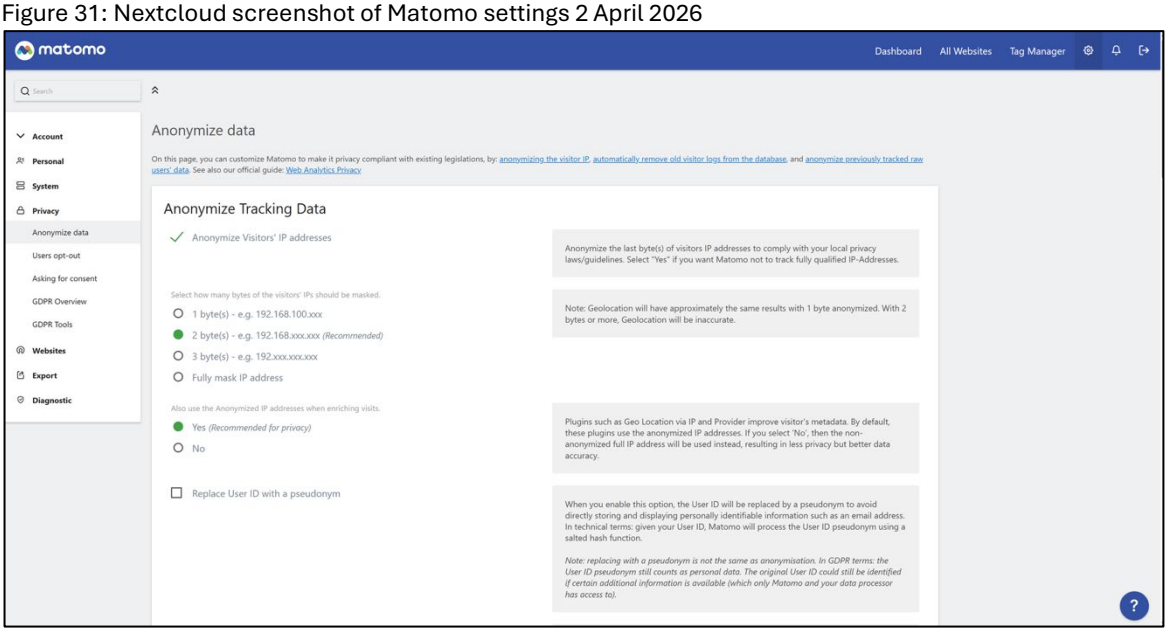
After testing, SURF filed two DSARs per email. Both the original request and reminder were addressed to a contact person from Nextcloud and to the official email address for DSARs, to Nextcloud's external privacy support by DataCo GmbH. Due to a misconfiguration on SURF's email server's side (the *Sender Policy Framework* was not correctly configured) nor DataCo nor Nextcloud received the mails from the end user, only the admin request. Nextcloud confirmed its own and DataGuard's mail servers do indeed refuse all mails from improperly configured mail servers. However, to help customers, Nextcloud decided to create a form to file DSARs. The form is accessible via Nextcloud's Privacy and Legal Policy.[111]

Nextcloud explains in its general Privacy and Legal Policy that this form helps website visitors gain access to their data: "*By using the button, all visitors of our website have the opportunity to make use of their data subject rights.*"[112]

In reply to the DSAR from the admin Nextcloud could not find any personal data about visits to Nextcloud's public or Nextcloud's restricted access websites, due to the short retention period of seven days. SURF also did not consent to the use of analytic cookies. If SURF had accepted the analytic cookies, Nextcloud would still have been unable to provide access, since Nextcloud's analytics tool (Matomo) immediately shortens the IP addresses. Nextcloud uses the functionality 'anonymise IP' from Matomo to remove the last two octets of the IPv4 addresses of visitors.[113] See Figure 31 below.

[110] Nextcloud, Cookies stored by Nextcloud, URL: https://docs.nextcloud.com/server/latest/admin_manual/gdpr/cookies.html
[111] Explanation Nextcloud in meeting with SURF and Privacy Company, 9 February 2026. The link to the form can be found in Section XXI of the Privacy and Legal Policy, *Your rights as a data subject*, URL: https://nextcloud.com/privacy/#h_21
[112] Nextcloud Privacy and Legal Policy.
[113] Matomo, FAQ, How does IP Address Anonymisation work in Matomo?, URL: https://matomo.org/faq/general/how-does-ip-address-anonymisation-work-in-matomo/ .

Figure 31: Nextcloud screenshot of Matomo settings 2 April 2026



A.3.6.1 DSAR response to the SURF test admin

Nextcloud responded to the test admin's DSAR on 23 December 2025 (within 8 days of submission) and returned several screenshots accompanied with a PDF explaining the data.

The PDF contains:

- Details about SURF's Nextcloud Enterprise subscription, with the Subscription ID, the fact the license is for a maximum of 20 users, and the 'Nextcloud Ultimate' bundle type. It states [name redacted by SURF for privacy] is the account manager and confirmed the subscription's start date as 4 November 2025 with a one-year duration;
- Interactions with the Zammad support portal (support.nextcloud.com), listing five specific support tickets. These tickets covered topics generated by default such as "Nextcloud Outlook Add-In" and "Nextcloud Talk High Performance Backend" , in addition to a request regarding the inability to add colleagues to the subscription (which SURF submitted). Nextcloud noted that session data, such as browser information and user location, are processed to provide functional features like the "Remember me" service, and that the processing is based on Nextcloud's legitimate interest in maintaining a functional website;
- Communication logs, primarily facilitated through the Postmark service. These logs included security updates related to the 'user_saml' and 'Tables' applications, as well as detailed correspondence regarding the DPIA assessment. The records showed a series of emails between SURF and Nextcloud in November and December 2025, including questions for the DPIA, weekly updates, and a follow-up meeting scheduled for January 2026. Furthermore, marketing logs revealed invitations to various webinars, such as those focusing on digital sovereignty, on-premises AI, and a comparison between Nextcloud Hub and Microsoft 365;
- A description of Nextcloud's legal base

- s for the processing of the personal data, including necessity to fulfil a contract (Art. 6(1) b of the GDPR) for managing support tickets and providing licenses through Sendent. Other activities, such as maintaining Zammad sessions for website functionality and sending webinar invitations, are performed under the legal ground of necessity for Nextcloud's legitimate interests (Art. 6(1) f of the GDPR);
- The names of 3 specific third-party processors involved in processing of the data, Zammad GmbH (support ticketing), ActiveCampaign LLC (for the Postmark emails service) and Sendent (license key distribution). Nextcloud also identified DataCo GmbH (Nextcloud's external privacy team) as recipient (but not as processor) of the personal data.[114]
- Regarding data retention, Nextcloud explained that session data are deleted upon logout or expiry, while support tickets and contractual data are kept for the duration of the relationship or as required by legal retention duties, such as tax and audit compliance. Generally, communication data are deleted after three years, and marketing data are retained until the user opts out;
- Nextcloud informed SURF of its statutory rights, including the right to rectification, erasure, and objection, and provided contact details for the supervisory authority in Baden-Württemberg (should SURF wish to make a complaint).

The response was detailed and easy to read. However, the reply was not always correct (any customer can always file a complaint with their national Data Protection Authority, customers are not required to contact an authority elsewhere in the EU), but more importantly, not complete.

SURF observed several potential omissions and asked Nextcloud to reply. Table 4 contains a description of the potential omissions and Nextcloud's reply. Based on SURF's assessment of these replies, Nextcloud's answer to the DSAR was fairly complete. Nextcloud convincingly argued it did not collect some of the apparently missing data or indicated it was willing to provide the (short lived) data in reply to a future DSAR, if the data subject provided additional data that could help Nextcloud reliably identify the data subject.

The missing data that Nextcloud should provide in reply to future DSARs are:

1. The Usage Survey Data - Nextcloud incorrectly claimed the report did not contain personal data, but can identify the admin via the IP address and the unique server instance ID
2. The session logs about use of the Support Portal (Nextcloud must ask Zammad to provide the contents from the production log)
3. Webserver access logs – Nextcloud should have 'frozen' the data relating to the requesting data subject in reply to the DSAR (provided the data subject was able to provide relevant IDs for Nextcloud to reliably verify the identity of the data subject)
4. Logs kept by Sendent (or other license provider) and Postmark (and future EU mail delivery provider).

[114] During the creation of this DPIA, Nextcloud contracted DataGuard as processor for the specific processing via a DSAR form, but this form was not yet available when SURF filed the DSAR.

Table 4: Overview of potentially missing data from DSAR and reply Nextcloud

Missing information about admin	Reply Nextcloud
Personal data such as IP address and possibly a pseudonymous identifier collected when downloading the software through the Nextcloud app hub (which may redirect to GitHub or Hugging Face)	Nextcloud logs downloads, including IP address and Enterprise Key, but cannot link those downloads to individual admins unless they provide additional identifying information. The retention period is only seven days. Where the download process redirects to third-party platforms (GitHub or Hugging Face), those platforms act as independent controllers for their own logging activities. In such cases, IP addresses or other identifiers processed by those third parties are not available to Nextcloud.
The contents and metadata relating to the Usage Survey shared by the admin from SURF's local Nextcloud instance with Nextcloud GmbH.	Nextcloud initially claimed the Usage Survey did not contain any personal data. Nextcloud wrote: *It is technical information about the installed apps and their version numbers and statistics like how many users the instance has, how many shares without further personal identifiers. The report does not include any user names or email addresses. Consequently, the Usage Survey does not contain personal identifiers of end users.*
	SURF disagreed with this analysis as evidenced in Section A.3.3.2. Later, on 20 January 2026, Nextcloud did share the Usage Survey SURF submitted after an additional email requesting access to these data.
Website Data. SURF distinguishes between the (relevant pages of the) publicly accessible website nextcloud.com and the restricted access websites support.nextcloud.com and portal.nextcloud.com (login required). Website Data are not limited to cookies, but include pixels, URL parameters and other similar technologies;	Nextcloud provided the session data from the support portal, but no (webserver access) logs. The support portal is hosted by Zammad. Zammad only provides session data to Nextcloud, nothing else. Only two people at Zammad have access to the production log. Portal.nextcloud.com does not collect any data but instead just connects to support.nextcloud.com and uses the same credentials. For portal.nextcloud.com there is no session/remember me cookie. Nextcloud explained: *Our website is using Matomo but all IP addresses are shortened immediately, so we have no possibility to make a connection to any of your (or* [the test admin's]*) sessions*.

	In addition, we reviewed relevant server and security logs for the defined period. Where data is only available in aggregated or anonymised form, they no longer constitute personal data and cannot be attributed to an individual. In a second reply Nextcloud added it only retains the webserver access logs for seven days and does not have other security logs or SIEM that store such data.
Authentication (login-logout) data from the Nextcloud Support Hub (support.nextcloud.com) and other logs, and the Portal (portal.nextcloud.com);	Nextcloud explained: "*We only have data of the currently active session (Nextcloud provided a screenshot with session data from Zammad). This contains when the current active session was started and when it was updated. But it does not keep track of previous sessions, there is no history*."
An explanation if the provided data are complete and reflect all personal data collected as a result of the performed tests, even if a) Nextcloud would have normally immediately deleted/anonymised such data, and/or b) if Nextcloud appeals to a specific legal exception allowing Nextcloud to not provide access to some personal data. This should also include the obvious, such as: "*Nextcloud does not provide access to the contents of support tickets because Nextcloud already makes these data available via the Support Hub*"	Nextcloud explained: "*We have conducted reasonable and proportionate searches across the systems that are relevant for the processing activities in scope and within the requested time period. Our DSAR reply includes the personal data relating to [the SURF admin] that are currently available to us and attributable on the basis of the identifiers provided. Where no personal data was located in a specific system for the defined scope, this indicates that either no such data was processed in that system for the relevant period, or the data is no longer available due to applicable retention, deletion, or anonymisation measures.* *For the DSAR reply we did not rely on a general legal exception to withhold personal data*."
An explanation of Nextcloud's GDPR role and the role of third parties engaged by Nextcloud. By referring to legal grounds in its reply to the DSAR, SURF assumes Nextcloud self-qualifies as data controller, at least for the support tickets, but this contradicts the role as processor based on the standard Enterprise DPA. It was unclear for data subjects if Nextcloud is the controller or the processor for the (other) personal data Nextcloud processes related to the	As processor Nextcloud uses two regular and two optional sub-processors : ○ Zammad – provision of the support portal support.nextcloud.com ○ ActiveCampaign provides the service called "Postmark", an email delivery service ○ Optional: Sendent – an optional technology partner who provided licenses to the SURF admin. As the license was bound to his email address, data was

Enterprise license. In addition, it is unclear what the GDPR role was of the 4 third parties Nextcloud mentions, one of which (Postmark), a US American company (ActiveCampaign, LLC).	transferred. They could have provided support, but didn't. ○ Optional: DataCo GmbH (DataGuard) for the new DSAR form Recipient DataCo GmbH ("DataGuard") supports Nextcloud with compliance and privacy related topics. DataCo GmbH is only a subprocessor with respect to the DSAR portal.
Any logs or personal data related to the mobile application push notification service (customerpush.nextcloud.com) initiated from SURF's Nextcloud instance and sent to mobile devices for user accounts admin and [test user]	Devices create the device ID locally and send it to the Nextcloud server of the organisation, so that the server can send push notifications to a user. These data are only in the customer's own Nextcloud server. Nextcloud GmbH only stores the device ID on its push proxy "*which cannot be traced back to any specific user as we do not have any further identifiers or reference data. If you provide the device ID, we could check whether this device ID is stored, and if so, we process the date on which the device was registered as well as the public key used for push notification delivery*."

Nextcloud has provided more detailed information to SURF about the data processing by Zammad, Sendent and ActiveCampaign (Postmark).[115]

Zammad does not provide a possibility to export session data. It is also not possible to export comments or tickets. Therefore Nextcloud provided a screenshot of the available recent session log of the interactions of SURF's test admin.

Sendent collects the email address and company name, plus an internal customer number and the count of daily active users from customers using Sendent (this count can differ from the number of Nextcloud users on a system). Customers already have access to these data themselves. If Sendent is involved, and the company provides support to a customer, it will use the Zammad support portal, so these data are included in the information about Zammad in reply to a DSAR. Therefore Nextcloud doesn't have to separately provide access to this information (but should describe in its reply to the DSAR where relevant that these data are processed by Sendent).

Postmark logs contain Message ID, Status (Delivered, Processed, Undeliverable), Email address, Subject, Tag (always empty), Date and Time, Bounce reason (if undelivered).

[115] Nextcloud answers 6 May 2026 to questions SURF 17 April 2026.

Postmark explains: "*By default, this activity data (including message content and related metadata) is retained for 45 days, after which the content and related metadata for delivered messages are deleted from our systems.*"

Mitigating measures Nextcloud:

- Nextcloud commits to provide a complete reply to a DSAR request from an admin, both in its role as processor, and its role as authorised controller (to the extent an individual can be identified as many of the authorised further processing purposes only involve aggregated data). This includes access to any collected Usage Survey Data, historical logs about the use of the Support Portal, frozen webserver access logs - provided Nextcloud can reliably verify the identity of the data subject, and logs kept by Postmark (or future EU based mail service provider).
- Nextcloud is actively looking for an EU-based mail delivery provider to replace the US American Postmark in Q3 2026.

A.4 Privacy Controls

The Nextcloud software includes relevant central privacy controls. When asked how Nextcloud ensures the application of privacy by design and privacy by default, Nextcloud answered it approaches privacy primarily through its core mission and the inherent sensibility of its developers, including the community of privacy conscious external developers, rather than through specific privacy technologists or explicit Privacy by Design documentation.[116]

A.4.1 Privacy controls for admins

The Technical Appendix describes 13 relevant privacy controls for admins in detail, including a missing control. Additionally, Section A.6.1 describes relevant security controls. In summary, the relevant privacy controls are:

1. Demand consent from all participants for the recording of meetings. In that case, users always get a pop-up with a consent request, even if the host does not want to record. This smoothes the process if a host decides to record the meeting after the start.
2. Hosts (but not admins!) can enforce use of the lobby, which means a room is locked except for admission by the host/moderator.
3. Change the default storage of recordings and transcriptions. By default these files are stored in the personal directory of the host/owner of the meeting, but organisations may want to have more control over access and deletion by storing recordings in a central location.
4. Set access rules for files based on roles/groups/geolocation regions (see for more details Section A.6.1.3).
5. Select what apps are available to end users: only 'supported apps' (that should be production ready) or also community apps.

[116] Nextcloud answers to questions SURF, 18 September 2025.

6. Enable Smart Picker and decide what (generally unsupported) third party integrations are allowed, such as emoticons, gifs and other “funny” interactions, integrations with GitHub, Reddit, Mastodon, etc.
7. Configure an organisation specific privacy policy and legal notice link.
8. Determine how end users share personal profile data, for example by enabling or disabling global autocompletion, which determines whether the system suggests users as a searcher types a name. Or by restricting a user’s search results to only those individuals within their own predefined department or team and by phonebook restrictions.
9. Enable users to use End to End Encryption in Talk and Files for confidential and sensitive data. Admins can also install the extension called Mailvelope to embed OpenPGP in Mail.
10. Enable watermarking and hiding of download options. If organisations allow users to share files with external users via Talk or Files, admins can allow users to add a watermark to help prevent unauthorised copying and create a hurdle for participants by hiding the download button .
11. Apply data retention controls. Admins can decide on the retention period of chats, and can change the default retention period of 28 days for rooms created from calendar invitation (via the ‘occ’ command). Admins can also use the combination of the Retention app and the Automated Tagging app to create rules for automatic deletion of files with specific labels, including recordings of videoconferences. See Section 3.1.11 in the Tech Appendix
12. Install the Data Request app to help end users exercise their data subject rights.
13. Missing control: prevent NSFW and NSFL profile pictures. SURF tested whether Nextcloud identifies, filters and blocks profile pictures and Talk group pictures uploaded by users for NSFW (Not Safe for Work) and NSFL (Not Safe for Life) content. SURF found that Nextcloud does not have any of such mechanisms in place, nor does any app exist suggesting this functionality. As such, users can configure any picture, regardless of its content. This is currently an open issue on Nextcloud’s GitHub page.[117] However, administrators do have the ability to delete contested users’ profile pictures in case of complaints by removing the picture from the user’s directory on the server.

Mitigating measures Nextcloud:

- Nextcloud will expand the ‘lobby’ feature (no. 2 in the list above) and enable admins to centrally enforce use of the lobby, via occ/appconfig from next major release onward (nc34).

A.4.2 Privacy controls for end users

The privacy configuration options for end users are limited, as most choices have been made centrally in the software itself (i.e. by Nextcloud), or by the admins of the education organisations. This section highlights 3 relevant options, related to:

[117] GitHub – Nextcloud – Issues – Allow Admin to add, remove, or replace profile images for users, URL: https://github.com/nextcloud/server/issues/49979

1. Content and visibility of profile data.
2. Exercise of data subjects' rights
3. App-specific options in Write

A.4.2.1 Profile data

Users can manage their account information and visibility preferences. The two key visibility options are:

1. **Attribute-Level Control:** Users can set individual visibility scopes for each profile attribute.
2. **Global Profile Visibility:** Users may restrict profile visibility to "logged-in users only" to prevent unauthenticated guests from accessing their profile information, regardless of individual attribute settings. Users also may change their status from 'Online' to 'Invisible', for instance, to appear offline to other users.

Nextcloud publicly provides some guidance about configuring and using Nextcloud in a privacy friendly manner in a user manual.[118]

A.4.2.2 Exercise of data subjects' rights

If the admin has installed the Data Request app, end users can exercise their data protection rights by asking the controller - the education organisation - for access, deletion or export of their data under the 'Personal Info' section of their personal settings.

A.4.2.3 Write specific settings

During testing, SURF observed two options in Write that have an impact on the data processing: the possibility to export comments in the margin, and the option to add personal data to the metadata of a document.

A.5 Data Processing Purposes

Education organisations can use the tested Nextcloud Enterprise software for many different purposes. To help privacy officers of the education organisations complete their own Register of Processing Activities (RoPA), Section A.5.1 includes a list of specific purposes for each of the tested core applications. Overall, organisations use productivity software (with remote web access) for the following 4 general processing purposes:

1. Facilitate (international) collaboration, information sharing and communication between employees and students in- and outside of the education organisation, including guest users
2. Reduce commuting/enable hybrid working
3. Provide first and second line support to employees and students
4. Use reports and logs for purposes such as maintenance, installing updates, troubleshooting, bug fixing and data breach detection/solution, in line with the organisation's internal IT policy.

[118] Nextcloud, User Manual, URL: https://docs.nextcloud.com/server/latest/user_manual/en/userpreferences.html. See also: https://github.com/nextcloud/server/issues/49979 .

The interests of education organisations in the use of the Nextcloud Enterprise software are described in Section A.8 of this report.

Section A.5.2 describes Nextcloud's purposes, as defined in the amended DPA with SURF.

Depending on the company's role as processor or as authorised controller, there are two different groups of purposes for which it processes personal data:

1. Purposes determined by the education organisation (Nextcloud as processor).
2. Authorised further processing purposes (Nextcloud data controller)
3. Purposes determined by Nextcloud (as independent data controller)

A.5.1 Detailed purposes Education organisations

Each individual education organisation must assess if people use the software to exchange special categories of data, as may be the case in, for example, job applications/CVs, assessments, interviews, research or mentoring sessions. In that case they must weigh the risks of unauthorised and unlawful processing, including excessive retention periods and oversharing. As described in Section A.3.6.1, admins can take technical measures to protect the data against data breaches, with more restrictive measures for confidential and sensitive data.

Write
- Writing assignments and instructions for students
- Preparing exams or tests
- Drafting internal (teaching) documents
- Providing feedback on student work

Spreadsheet
- Keeping grade overviews, recalculating averages
- Tracking attendance or participation
- Setting up daily, weekly and yearly calendars
- Collaborating with colleagues

Talk
- Conducting audio and video calls, including chat
- Presenting materials through a shared screen during video calls
- Communicating with students via chat
- Communicating with colleagues about teaching activities
- Sharing class-related files with students (and other teachers)
- Holding online classes
- Collaboration during meetings with a whiteboard, chats, polls and AI-transcription (minutes).

Mail
- Communicating course-related information to students
- Answering student questions
- Communicating with colleagues (about teaching and planning)

- Sending instructions or feedback to students
- Sending reminders related to classes or deadlines

Present
- Creating presentations for lessons/lectures/internal management purposes
- Updating existing teaching presentations

Files
- Storing teaching materials
- Accessing teaching materials from different locations
- Sharing documents/presentations with students
- Sharing documents with internal and external colleagues
- Collaborating on documents (teaching materials)

A.5.2 Purposes Nextcloud

As mentioned in the introduction of this Section 5, there are two different groups of purposes for which Nextcloud currently processes personal data, depending on its self-qualification as processor or controller.

Each supplier of software and services also needs to process some, generally aggregated, personal data for its own legitimate business purposes, such as billing. To ensure control over this data processing, SURF has proposed to Nextcloud to distinguish a third category of processing purposes: authorised 'further processing' of personal data for specific purposes as data controller. The authorisation for this further processing for these purposes is necessary to prevent Nextcloud as a processor from unlawfully taking decisions about the purposes of the processing, and hence becoming a controller (article 28(10) GDPR). See the factual analysis of the legal role of Nextcloud in Section A.7 below.

A.5.2.1 Processor purposes

In the amended DPA, Nextcloud and SURF have agreed on a limitative list of four processing purposes for Nextcloud as data processor. These purposes are:

1. Technically provide the Software and applications via portal.nextcloud.com (Process visitor and download information);
2. Provide third level support/technical assistance based on third line requests from Customers;
3. Help secure Personal Data Processed by the Customer in the Software by sending update notifications and newsletters about technical updates and security developments to admins;
4. Technically improve the Software and Services for all Customers, including bug fixing, troubleshooting, patching, and general maintenance by using the aggregated Support and voluntarily provided Diagnostic Data.

SURF and Nextcloud have also agreed to list specific purposes for which Nextcloud shall not process any personal data:

1. Nextcloud shall not process Personal Data for any “further” or “compatible” purposes (within the meaning of Articles 5(1)(b) and 6(4) GDPR) other than those specified in this DPA or enabled by the Customer account administrator.
2. Nextcloud will not Process Personal Data for advertising purposes or serve advertising in the software and services and Nextcloud will not process Personal Data for direct marketing, profiling, research or analytics purposes except where such processing is necessary to comply with Customer’s Instructions (commercial mailings to procurement officers, if the customer has not opted-out).
3. Nextcloud will not Process Personal Data for content scanning or monitoring purposes, including scanning for Child Sexual Abuse Material (“CSAM”).

Furthermore, SURF and Nextcloud have agreed on a limitative list of legitimate business purposes for which Nextcloud may *further* process the data it collects as an authorised controller (see Section A.5.2.2 below). The agreement on these two lists of purposes and excluded purposes has consequences for the legal role of Nextcloud as processor or controller. See the factual analysis of the legal role of Nextcloud in Section A.7 below.

A.5.2.2 Legitimate business purposes (authorised data controller)

Nextcloud has agreed to include a list of seven Legitimate Business Purposes in the amended DPA with SURF, that is, authorised *further processing* of personal data, aggregated where possible, for Nextcloud’s own legitimate business purposes, when the processing is strictly necessary. Nextcloud qualifies as controller for the processing for these purposes.

The agreed purposes are:

1. Comply with legal obligations. This includes responding to requests from government authorities for compelled disclosure, under specific conditions, and answering Data Subject requests for Personal Data Processed by Nextcloud as Authorised Controller.
2. Use Commercial Contact Data, number of procured licenses and Customer identifying data for billing, fulfilling of orders and receiving payments, not for other commercial purposes.
3. Process Commercial Contact Data for Customer relationship management, including the sending of commercial mailings.
4. Process Diagnostic Data (user statistics) for the detection of licensing compliance and fraud detection and prevention, including possible inspection of End User license data in case of an in situ audit.
5. Process statistical Diagnostic, Support and Website Data for internal reporting, financial reporting and product strategy, including for prioritising security patches and feature development calendars.
6. Create statistical Website analytics (including receiving analytics related to Software downloads from external repositories) from the (relevant pages on the) restricted access support and management portals (support.nextcloud.com and portal.nextcloud.com).
7. Technically improve and optimise the performance and efficiency of the Software, support Services and Nextcloud’s internal IT infrastructure by using statistical Support, Diagnostic and Website Data.

Nextcloud may only process personal data for these legitimate business purposes when the processing is strictly necessary and proportionate for one of these purposes. The amended DPA explicitly prohibits Nextcloud from determining any other compatible or *further processing* purposes, and prohibits Nextcloud from processing personal data for advertising purposes or to serve advertising in the Software and Services, for direct marketing, profiling, research or analytics purposes, except where such Processing is necessary to comply with Customer's instructions (such as a subscription to a commercial mailing).

Absent such a list and restrictions, it is plausible that the education organisation and Nextcloud would factually qualify as joint controllers.[119] This argument about joint controllership will be explained in more detail in the factual analysis of the legal role of Nextcloud in Section A.7 below. The new list includes a specification of the two purposes *optimise* and *further develop* that are part of Nextcloud's current publicly available template DPA.

Two of the seven agreed further processing purposes are explained in more detail below: compliance with legal obligations and checks on licensing compliance.

Comply with legal obligations

Nextcloud may be ordered to disclose the -limited - personal data it collects pursuant to requests by courts or government agencies, such as law enforcement authorities. Even though Nextcloud GmbH as a German company under exclusive German ownership is in principle not subjected to non-EU law or jurisdiction, Nextcloud may be ordered by government authorities, agencies or courts within the EU, or parties that can invoke EU law, to disclose the limited personal data it has about its customers. Nextcloud added in reply to part A of this DPIA that it doesn't have access to any data processed by customers in their self-hosted environment, or environments managed by partners.[120]

Nextcloud does not explicitly address the legal obligation to disclose personal data in its Privacy and Legal Policy, only implicitly when it refers to legal obligations to retain data. If Nextcloud provides support and maintenance services to customers outside of the EU, it may have to comply with member state, EU and foreign trade laws and sanction decisions. It follows from public sources that there are companies in the USA that use the Nextcloud software.[121] It is unclear if Nextcloud also sells Enterprise licenses to these companies.

Based on the known facts about the US sanction decisions against members of the International Criminal Court, and against European Commissioner Thierry Breton, such decisions effectively force US American companies, including foreign branches and subsidiaries [see for example EOP 14203, sec. 8(c)], to stop servicing targeted individuals and organisation, while they may or may not appeal the decision. Though such decisions cannot apply to Nextcloud when it services EU-based customers, there is a (small) chance

[119] Nextcloud was concerned that the inclusion of this list of authorised purposes could be interpreted as an 'instruction' from the controllers to Nextcloud as processor. The DPA therefore specifies that Nextcloud is nor a processor, nor a joint controller when processing personal data for these seven legitimate business purposes.
[120] Nextcloud reply to part A of the DPIA, 2 April 2026.
[121] TheirStack, Companies that use Nextcloud in United States, undated, URL: https://theirstack.com/en/technology/nextcloud/us (last visited 16 February 2026).

that the USA could put the entire company Nextcloud GmbH on one of its sanction lists if it continued to provide services to a sanctioned person or organisation in the USA or elsewhere. Such a sanction would ban US customers from purchasing Nextcloud Enterprise services, and thus economically blackmail Nextcloud in compliance with extraterritorial law.

In reply to this analysis Nextcloud answered:
"It is theoretically possible that a foreign government — including the US — would attempt this, but the impact would be limited, for two reasons.

First, our company is structured to minimize the impact of such a move on our customers. Operational responsibility lies with the customer or a Nextcloud partner. Nextcloud provides security services, support, and access to the enterprise build, but has no direct access to the operational service at the customer. This isolates the customer from immediate impact in the unlikely event of a forced cessation of services.

Second, Nextcloud GmbH could not afford to comply with a demand from one government if it affected customers in other regions. Two facts drive this: our customers deploy our product specifically to protect their operations from interference by foreign governments, and our revenue is spread globally.

It follows that complying with an extraterritorial demand — one made by an authority in one country but affecting customers in another — would seriously damage our business by undermining its core value proposition. The realistic response, both legally and commercially, would be to refuse and instead cease operations in the country making the demand." [122]

Even though the nature and volume of personal data Nextcloud processes is limited, certainly in comparison with providers of cloud productivity services, SURF proposed to add specific conditions about Nextcloud's compliance with legal orders to the DPA. As processor, Nextcloud must conduct a thorough legal review of any request if it is prohibited from forwarding the request to the customer, and object to the request as a matter of principle (since as a processor Nextcloud should first avoid ending up in a situation where it has to take decisions about disclosure, as a form of data processing).

As confirmed by the EDPS in its March 2024 decision on the use of Microsoft 365 services by the European Commission[123], in those circumstances, Nextcloud acts as a data controller, to comply with legal obligations.

The EDPS wrote:
"*When Microsoft processes personal data in order to comply with its legal obligations, such processing cannot be considered as effectively falling within the provision of online services and is not carried out on the Commission's behalf.*"[124]

[122] Nextcloud reply in an email from 7 July 2026.
[123] EDPS decision on the investigation into the European Commission's use of Microsoft 365, 8 March 2024, par. 183, URL: https://www.edps.europa.eu/system/files/2024-03/24-03-08-edps-investigation-ec-microsoft365_en.pdf.
[124] Ibid.

If Nextcloud is compelled to disclose personal data, to a court, law enforcement authority, security agency or secret service outside of the EU, it factually takes a decision about the purpose of the processing, and hence, acts as controller. To prevent unintentional joint controllership, this purpose of compliance with legal obligations was included in the list of 'authorised' further processing purposes (Nextcloud as 'authorised' controller).

Licensing compliance
Nextcloud describes in its Enterprise Terms and Conditions that it processes license information data for the detection of licensing compliance and fraud detection/prevention. Customers must also keep records of license use. As explained in Section A.3.4, Nextcloud collects information about license data via the Support App and via the Usage Survey. If customers do not use the Support App, Nextcloud "*reserves the right to conduct an audit of the customers' records in case there are reasons to suspect the customer is breaching the license agreement by having more users than paid for*."[125]

A.5.2.3 Purposes independent data controller

In its Terms and Conditions for Nextcloud Enterprise and its general Privacy and Legal Policy (applicable to all customers) Nextcloud mentions many processing purposes related to the use of the software that are no longer relevant for SURF-members, as Nextcloud will either act as processor or as authorised controller for these purposes.

However, Nextcloud remains an independent data controller for the data collection via Nextcloud's public websites, data processing via reported problems sent to abuse@nextcloud.com and communication with prospective customers, via for example events, social media and the public Nextcloud Forum.

A.6 Open source & security

Nextcloud GmbH does not offer software-as-a-service (SaaS) itself. Enterprise customers have to host the software themselves, and hence, take responsibility for the security of the hosting infrastructure, or engage a Nextcloud hosting partner for a fully managed solution. Nextcloud helps its Enterprise customers secure the data processed by the software by regularly offering new versions of the software, both as major new versions, and as maintenance releases.[126]

However, different from well-known cloud suppliers of productivity software, Nextcloud does not have its own global security centre that monitors 24/7 for network and infrastructure attacks. To protect the data processed on the self-managed servers against unauthorised access, education organisations need to implement their own security guardrails, and include the Nextcloud servers in their existing Security Information and Event Management tools (SIEM).

Also different from its competitors, Nextcloud is 100% open source. This has security benefits, because every code developer in the world can check the code for bugs and possible backdoors, and disclose such security risks (preferably via the Coordinated

[125] Nextcloud reply to part A of the DPIA, 2 April 2026. This condition is not yet included in the Terms and Conditions or in the DPA.
[126] Nextcloud, Maintenance and release schedule, undated, URL: https://docs.nextcloud.com/server/stable/admin_manual/release_schedule.html (last visited February 2026).

Vulnerability Disclosure – CVD procedure).[127] At the same time, the open source character of the software also enables malicious actors to develop attacks on educations' self-managed systems without triggering any security flags at Nextcloud.

The Nextcloud software is licensed under the GNU AGPLv3, the specific version for network interaction with software. The license is based on GPL, one of the most widely used Open Source licenses. The AGPLv3 includes an additional right that if the program is expressly designed to accept user requests and send responses over a network, the user is entitled to receive the source code of the version being used. [128]

The license is often qualified as 'copyleft' since it enables rather than prohibits use of code. Developers can file patent claims for the code (system and method) they develop, but under this license they automatically grant all users a non-exclusive, non-transferable, worldwide, royalty-free license on any patents. This doesn't mean that everybody can just grab great work developed for a common good and privately exploit that work in a new proprietary context. If others create derivative works, these works must also be released under the AGPL license. Otherwise, the new work results in a copyright or patent infringement that the developer can take legal action against.
The AGPLv3 license is thus designed to guarantee that all users of the software can use, study, share and improve the software without risking potential violations of copyright or intellectual property rights.

Nextcloud GmbH itself also guarantees that every customer can use Nextcloud and exercise all rights given by the GNU AGPLv3 without violating any patents or copyright. This extra guarantee provides an important assurance for data sovereignty. Even if Nextcloud would be bought by a (non-EU based) competitor, nor Nextcloud nor the new owner can undo the open source nature of the software, and the copyleft assurance. In such circumstances, the open source development community is likely to create a 'fork', and start with the further open source development from that specific version onwards.

In 2017 Nextcloud has self-certified its compliance with the GNU AGPLv3 conditions drafted by OpenChain, a Linux Foundation project.[129] Since, OpenChain has translated these conditions in two standards, for open source license compliance (OpenChain ISO/IEC 5230) and open source security assurance (ISO/IEC 18974). Nextcloud does not have certifications for compliance with either of these two international standards.

To help education organisations assess the security of the open source Nextcloud software, SURF has performed a separate security assessment. The main outcomes of this assessment are included below.

The scope is limited to the (tested) software provided by Nextcloud, including Collabora Online from the UK company Collabora. SURF's security assessment does not replace a BIO assessment and education organisations that wish to deploy Nextcloud should still perform their own security assessment for the hosting and infrastructure.

[127] Report vulnerabilities, URL: https://hackerone.com/nextcloud.
[128] Free Software Foundation, The fundamentals of the AGPLv3, fall 2021, URL: https://www.fsf.org/bulletin/2021/fall/the-fundamentals-of-the-agplv3.
[129] Nextcloud Validates License Compliance Through OpenChain, 6 June 2017, URL: https://nextcloud.com/blog/nextcloud-validates-license-compliance-through-openchain/

A.6.1 Security Assessment Findings

SURF performed a security assessment through a review and analysis of documentation provided by the vendor as well as publicly available information from the open source developer community (including project repositories and related materials on GitHub). The review focused on the implemented technical and organisational measures to protect the confidentiality, integrity and availability of data processed by the Nextcloud software.

This assessment is documentation-based and does not include a source code review, penetration testing, vulnerability scanning, or any other active attempts to identify exploitable vulnerabilities or to create data breaches. Furthermore, SURF did not perform an on-site audit.

The evaluation considered the adequacy and maturity of controls across the following security domains:

1. Assurance certifications
2. Encryption
3. Authentication and access control capabilities
4. Release and patch management
5. Support (long term and incidents)
6. Secure coding
7. Vulnerability management and CVE disclosure
8. Logging and auditing features
9. Software integrity and backdoor prevention

The outcomes of the assessment are summarised in subsections A.6.1.1 through to A.6.1.9 below.

A.6.1.1 Assurance Certifications and audits

Nextcloud has obtained a CSPN (Certification de securité de premier niveau, or First-Level Security Certification) certification from the ANSSI (Agence nationale de la sécurité des systems d'information) for the audit on Nextcloud Enterprise Files[130] Nextcloud has provided an earlier draft version of the audit report to SURF. The certificate was awarded in April 2026.[131]

The scope of the CSPN certification is limited to secure storage, but the (draft) report also mentions authentication , access control rules, secure communication as evaluated security features of the software. Currently, over 50 organisations have obtained certifications, sometimes for multiple software products.[132]

The CSPN serves as an alternative assessment method to the more comprehensive Common Criteria (CC) certification. CSPN specifically focuses on evaluating a products

[130] ANSSI, Rapport de certification ANSSI-CSPN-2026/03 Nextcloud Files Version 31.0.7.2 hébergement on-premise, URL: https://messervices.cyber.gouv.fr/visas/ANSSI-CSPN-2026-03-rapport.pdf.
[131] ANSSI, CSPN certification Nextcloud Files, 10 April 2026, URL: https://messervices.cyber.gouv.fr/visas/ANSSI-CSPN-2026-03-certificat.pdf.
[132] ANSSI PDF with a list of products with certifications, July 2026, URL: https://messervices.cyber.gouv.fr/visas/catalogue-produits-services-profils-de-protection-sites-certifies-qualifies-agrees-anssi.pdf

resistance to moderate level cyber-attacks. The CSPN evaluation consists of two main parts:

1. Compliance analysis, verification of the alignment of security functions with established criteria, and
2. Vulnerability analysis, the assessment of the resilience of those functions against potential circumvention by skilled attackers.

The evaluations for CSPN can only be performed by third-party organisations approved by ANSSI as Centre for the Evaluation of Information Technology (CESTI).[133] The certification has to be renewed every 3 years.

ANSSI has signed an agreement with its German counterpart, BSI, for mutual recognition of CSPN and BSZ (Accelerated Security Certification) schemes. This mutual recognition in two European countries eliminates the need for manufacturers to undergo multiple certification procedures in different markets for open source software, reducing costs and commercial barriers.[134]

Nextcloud's software was also audited in 2024 by the German national cybersecurity service BSI.[135] The audit report assesses the security of the Nextcloud server application and the extensions two factor admin support, two factor email, two factor TOTP provider, and two factor webauthn. BSI subjected the applications to comprehensive toll-based static source code analysis and an accompanying dynamic analysis. The investigation used a white box method, where testers had access to both the code and the running instances. The researchers found that the Nextcloud server application had security vulnerabilities of **medium to high** criticality. Malicious actors could exploit these vulnerabilities to compromise specific users and the application.

The comprehensive static source code analysis resulted in a total of two SAST findings classified as [medium] and 39 classified as [info], as well as 16 SCA findings classified as [high] and 6 as [medium]. The most important vulnerabilities related to authentication, and the possibility to bypass two factor authentication (2FA) on the self-hosted software.

The audit report explains that it is (was) possible to bypass 2FA verification by intercepting and manipulating the 2FA verification request. This allowed an attacker who obtained the login credentials for an account to compromise that account, even if 2FA was enabled for that account.

The audit report also describes a vulnerability relating to the use of multiple Nextcloud instances. Users can share files between instances, but there was no authentication mechanism between the exchanging instances. This means that receiving instance A could

[133] ANSSI product certification, page undated, URL: https://cyber.gouv.fr/offre-de-service/solutions-certifiees-et-qualifiees/comprendre-levaluation-de-securite/certification-de-produits/comprendre-la-certification/ . Currently 10 audit organisations are approved, see https://cyber.gouv.fr/offre-de-service/solutions-certifiees-et-qualifiees/evaluer-les-produits-et-services/centres-evaluation/centres-evaluation-cspn/ (pages last visited 17 February 2026).
[134] Systerel blog, First Level Security Certification (CSPN): The S2OPC Case Study, 12 May 2024, URL: https://blog.systerel.fr/posts/2024-05/certification-cspn-de-s2opc/
[135] BSI, Ergebnisbericht Security Quellcodeanalyse und Penetration Test, Projekt 604 – Codeanalyse für Opensource Software (CAOS3) Analyseergebnisse Arbeitspaket 2: „Nextcloud" 19.07.2024, Version 1.0, Status: Final, URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/P486-Codeanalyse/Nextcloud-Server.pdf?__blob=publicationFile&v=4.

not verify who the owner of the shared file was on the part of instance B. A user of instance B could therefore exchange a file with a user of instance A and pretend to be any user of instance B. An attacker could thus abuse the trustworthiness of another user of the attacker's instance to share malicious files with users of another instance. The only hurdle for sharing was a consent requirement: the attacked user ad to accept the request to share the file. This was not effective, since the attacker is posing as a trusted person and could hence easily obtain the consent of the attacked user.

The audit report describes other vulnerabilities relating to abuse of credentials used for external storage, not summarised here. SURF could not find public documentation if Nextcloud had solved these vulnerabilities. However, in reply to this DPIA Nextcloud explained that it had indeed solved all vulnerabilities. Nextcloud did publish (the mitigation of) the high vulnerability and explained it had already mostly fixed other vulnerabilities before BSI completed its report.[136]

Mitigating measures Nextcloud:

- In the amended DPA with SURF, Nextcloud has committed to renew the CSPN certification every 3 years.
- Nextcloud has solved the vulnerability of the 2FA verification on the admin portal (portal.nextcloud.com).
- Nextcloud has worked with its support ticketing provider Zammad to introduce 2FA on the support portal. Zammad has committed to Nextcloud to be able to enforce 2FA in the new version v7.1 which as been released 1 July 2026.

A.6.1.2 Encryption

The EDPB defines encryption as "*a process which consists of converting the information into a code in order to prevent unauthorised access. That information can only be read again by using the correct key. Encryption is used to guarantee the confidentiality of data. Encrypted data is still personal data. As such, encryption can be considered as one of the pseudonymisation techniques.*"[137]

Encryption can protect information both while it is being sent over networks (encryption in transit) and while it is stored on devices or servers (encryption at rest).

Roughly summarised, Nextcloud offers 3 types of encryption.

1. To protect data in transit (Nextcloud supports TLS for data in transit),[138],
2. As server-side encryption, where data are encrypted on the server and the server manages the keys (general or individual keys),

[136] GitHub, Ability to by-pass second factor, URL: https://github.com/nextcloud/security-advisories/security/advisories/GHSA-9v72-9xv5-3p7c , GitHub, fix(config) Make sure user keys are strings#44276, URL: https://github.com/nextcloud/server/pull/44276 NIST, CVE-2024-37313 Detail, URL: https://nvd.nist.gov/vuln/detail/CVE-2024-37313, GitHub, fix(config): Make sure user keys are strings#44276, URL: https://github.com/nextcloud/server/pull/44276

[137] EDPB Data protection guide – secure personal data https://www.edpb.europa.eu/sme-data-protection-guide/secure-personal-data_en

[138] Nextcloud, Server-side encryption configuration, page undated, URL: https://docs.nextcloud.com/server/latest/admin_manual/configuration_files/encryption_configuration.html (last visited seven February 2026).

3. As client-side encryption, where data are encrypted on the user's device before being sent to the server. This is End-to-End Encryption (E2EE) or zero knowledge: only the communicating devices can decrypt the data, the server cannot access the content data in readable form at any point.[139]

Nextcloud provides detailed information about the use of TLS and SSL to encrypt the web traffic.[140]

Nextcloud's Server-Side Encryption (SSE) is intended to safeguard the content of files stored on Nextcloud's server itself and on external storage locations. The protection exclusively applies to data at rest, meaning when files are stored and not actively accessed or processed by an authorised user. File and Folder names, as well as file previews and full text search indexes remain unencrypted. Though Nextcloud mentions object storage prevents direct leakage, metadata exposure remains a potential risk. Admins should disable features such as previews or search indexes in environments handling highly sensitive or confidential personal data.

Within SSE Nextcloud has implemented two options to create the keys: centrally, or per user.

In the server key approach the (central) master key is stored and managed on the customer's server, in configuration files (config.php). If the server is stolen or compromised, malicious actors can access the keys in the config file and decrypt data. By default, Nextcloud provides encryption with an internal ID. Nextcloud warns that use of the encryption app does not protect the customer's data if the Nextcloud server is compromised and that the encryption does not prevent Nextcloud administrators from reading users' files.

Alternatively, organisations can decide to create the keys per user, based on that user's password. In that case only the user can decrypt the files. The cryptographic key is stored in encrypted form when user is not logged in. Upon successful authentication the key is decrypted using the user's password and made available as part of user's active session. This approach enhances confidentiality compared to the server key model, as it limits the impact of server level compromise and reduces reliance on a centrally stored master key. In the event of stolen hardware or unauthorised access, only encrypted content would be accessible, and decryption would require the respective user's password.

However, during active file access, the decrypted key temporarily resides in the server memory. A sufficiently advanced malicious administrator with full and unrestricted access to the server environment could theoretically intercept keys during this runtime process. This risk is primarily associated with insider threats or full system compromise scenarios.

Other disadvantages are:

[139] Technically, E2EE is not possible for communication with a browser, but Nextcloud offers encryption for browser sessions nonetheless.
[140] Nextcloud, enabling ssl, page undated, URL: https://docs.nextcloud.com/server/latest/admin_manual/installation/source_installation.html#enabling-ssl and for nginx, URL: https://docs.nextcloud.com/server/latest/admin_manual/installation/nginx.html (pages last visited 17 February 2026).

- if users lose their password, or resign without decrypting, encrypted data can be permanently lost.
- the dependency on owner login for key updates
- every password change requires corresponding key updates.

In a whitepaper on server side encryption from 1 June 2025, Nextcloud provides detailed information about the process of generating keys, sharing , encrypting and decrypting files. [141] The description is consistent with established cryptographic best practices and provides strong protection for data at rest.

Nextcloud writes that its SSE employs cryptographic technologies and standards like OpenSSL and AES 256 which are commonly recognized as strong encryption mechanisms when properly implemented and configured. According to Nextcloud (but not tested by SURF), the SSE should scale effectively in large enterprise environments including deployments involving high user volumes and large file sizes.

Nextcloud also provides a whitepaper on client side end to end encryption (E2EE), with detailed instructions for admins.[142] The whitepaper was updated in March 2026 and accurately reflects Nextcloud's latest technology and process.

A.6.1.3 Authentication and access control capabilities

Authentication ensures that each user confirms their identity before accessing any system or personal data. The system assigns a unique identifier to each user, which then verifies their identity using credentials such as passwords, security tokens, or biometric factors. The EDPB recommends multi factor authentication: "*a user's authentication is considered strong when it uses a combination of at least two of these categories.*"[143]

Nextcloud writes in its whitepaper on security and authentication that it enables administrators to control file access and sharing through group based permissions. The system respects the access rights of underlying storage, and allows users to define approval workflows so that designated individuals can validate or reject newly submitted files prior to making them available. As per the white paper, administrators can implement fine grained file access controls to enforce business and legal requirements. These controls allow restrictions such as preventing access to XLSX files from the HR department by outside company IP ranges or blocking non EU countries from accessing customer data stored in Europe.

Nextcloud writes it supports the following authentication mechanisms:

1. LDAP/Active Directory integration, which lets users login with their company credentials.
2. Kerberos/ Oauth2/OpenID connect: these support login through trusted external identity systems.

[141] Nextcloud Whitepaper: Server-side encryption, securing data at rest, undated (Last accessed 16 February 2026)
[142] Nextcloud Whitepaper: End-to-end encryption design, March 2026, URL: https://nextcloud.com/c/uploads/2022/03/Nextcloud-end-to-end-encryption-Whitepaper.pdf
[143] EDPB data protection guide-secure personal data, Technical measures, undated, URL: https://www.edpb.europa.eu/sme-data-protection-guide/secure-personal-data_en#toc-1 (last visited 18 February 2026).

3. SAML 2.0/Single Sign On(SSO) , which allows users to login once and access system without a separate password.
4. Two-factor authentication Universal 2nd factor(U2F) and time based one-time password (TOTP) second factor, to increase login security.
5. REST style provisioning API, this allows to create and configure user accounts.
6. Supports creating guest accounts with limited access.

SURF did not test any of these options. Nextcloud provides a dedicated user management section in its documentation outlining configuration and support for these features.[144]

The software also includes brute force protection feature, a mechanism to protect the system against attempts to guess user passwords/tokens. This applies to sensitive entry points across Nextcloud's ecosystem. When the system detects repeated failed attempts from a specific IP address, it progressively slows down subsequent requests from that IP for up to 24 hours. In extreme cases, it can also block access from the IP for up to 30 minutes. Nextcloud publishes additional details and guidelines with important user information in the Nextcloud server administration guide.[145]

Nextcloud has written a whitepaper on security and authentication, but this does not include any information on role-based access control (RBAC). This omission is also mentioned in an open issue on Nextcloud's GitHub repository: users and developers have raised concerns about absence of this feature.[146] Nextcloud has confirmed to SURF it does not provide RBAC as such. However, Nextcloud wrote that its combined user and group based access controls can achieve the same purpose as RBAC.[147] Access control is implemented through users and groups, where permissions are assigned at group level across applications and features. Users are added to one or more groups, access to functionalities is granted or restricted based on group membership. Access to applications or features can be made exclusive or limited to specific user groups, where only selected groups are granted access while others are excluded based on the group membership.

SURF confirms that the group based access control model provides functional equivalence to RBAC in enforcing access restrictions. However, the model introduces operational inefficiencies due to the absence of a role based abstraction layer and reliance on direct user-to-group assignments. In RBAC, user access is managed through role assignment, where for instance , a single role change automatically updates all associated permissions. In the group based model scenario by Nextcloud, the same change requires updating user membership across one or more groups individually, as access is distributed across group and application level assignments. This could introduce operational overhead due to absence of a centralised role abstraction and reliance on multiple group-level updates for managing user access changes. In reply to this observation Nextcloud explained the assignment of users to a group is managed via an LDAP or AD. So when a user changes role, group membership is changed via that central directory.

[144] Nextcloud user management documentation Authentication, undated, https://docs.nextcloud.com/server/latest/admin_manual/configuration_user/authentication.html# (last visited 18 February 2026).
[145] Nextcloud admin manual Brute force protection, undated, https://docs.nextcloud.com/server/latest/admin_manual/configuration_server/bruteforce_configuration.html (last visited 18 February 2026).
[146] GitHub Nextcloud server issues https://github.com/nextcloud/server/issues/19903 GitHub Nextcloud server issues https://github.com/nextcloud/server/issues/19903 and https://github.com/nextcloud/server/issues/7482
[147] Nextcloud reply to part A of this DPIA, 2 April 2026.

In reply to questions from SURF, Nextcloud confirmed that its group based access control assigns the same rights to all users in a group. An admin can however decide to give advanced permissions to an individual user (a 'team folder manager'). The permissions apply to each group. If a user is a member of multiple groups, and has different access levels in the different groups, access is determined by the group settings, not by the user. To prevent oversharing to former employees, admins can assign temporary access to a group by setting an expiration date. Nextcloud also offers a retention feature on user accounts, to disable a user past a certain amount of time.

Nextcloud applies suspicious login detection on the server to protect the data against unauthorised access. See Section 4.4 in the Technical Appendix. Nextcloud explains:

"The Suspicious Login Detection app tracks successful logins on the instance for a set period of time (default is 60 days) and then uses the generated data to train a neural network. As soon as the first model is trained, the app starts classifying logins. Should it detect a password login classified as suspicious by the trained model, it will add an entry to the suspicious_login table, including the timestamp, request id and URL. The user will get a notification and the system administrator will be able to find this information in the logs.

When the user is notified, they can go to the security section in their user settings, terminate the suspicious session, and proceed to set a new password. The administrator can also take action, like disabling user accounts or forcing users to pick a new password."[148]

A.6.1.4 Release and patch management

Nextcloud documents its release and patch management via its own website[149] and publishes a maintenance and release schedule on GitHub.[150] SURF assesses this documentation as adequate. The activity within the community is pretty good, frequent and up to date.

Nextcloud only performs updates and releases patches for its officially supported apps. Enterprise customers have to carefully consider if they allow use of community apps. Nextcloud does not perform code reviews or other types of security validations. Nextcloud explained to SURF:

"*The tools for customers to check community apps provided by Nextcloud are: ratings on the apps by the community, which could help with deciding whether an app is trustworthy or not. As well as the fact they're open source. There are no additional (technical) tools provided by Nextcloud to aid in validating apps.*"[151]

Nextcloud explains: "*While community contributions can be incorporated into the core and maintained by Nextcloud, simply looking at the owner listed in the app store (""Nextcloud*

[148] Nextcloud blog, 25 April 2019, URL: https://nextcloud.com/blog/nextcloud-16-becomes-smarter-with-machine-learning-for-security-and-productivity/.
[149] Nextcloud, Maintenance and release schedule, page undated, URL: https://docs.nextcloud.com/server/latest/admin_manual/release_schedule.html (last visited seven February 2026).
[150] GitHub Nextcloud Maintenance and release Schedule , page undated, https://github.com/nextcloud/server/wiki/Maintenance-and-Release-Schedule (last visited February 2026)
[151] Nextcloud reply to technical questions SURF, 18 September 2025.

GmbH"") is not the sole indicator of support. Customers with a Nextcloud enterprise license can directly see which apps are covered under their support contract within the app store. Community users don't have this insight."[152]

Nextcloud also explained community apps may share data with third parties: "*For community apps, Nextcloud GmbH is not responsible of what the community apps are doing. It is the responsibility of the user to check whether or not the apps send data to third-parties. Usually, developers clearly indicate which third-parties are involved. But Nextcloud GmbH is not accountable for community apps which would send data to third-parties. Of course, the fact that apps are open-source helps reveal that an app is malicious*."

Nextcloud explained to SURF it carefully reviews its supported apps (see also Section A.6.1.6 below), and clearly informs customers if a third party is involved (such as for example external AI providers). "*Also, Nextcloud GmbH is accountable for any apps falling into the scope of support, so there is always careful development reviews to ensure that no malicious code, a fortiori no code that sends data to third-parties, is included in pull requests.*"[153]

Nextcloud describes it releases monthly maintenance versions for the server software, and quarterly major releases for the supported apps and software.[154]

"*We commit to monthly maintenance releases that address security issues and critical bugs for all supported major versions. Major releases occur ~every 16 weeks, with enterprise versions following 4–6 weeks later for added QA.*"[155]

"Critical fixes are backported during a 12-month support window per major version; enterprise support can extend this to 5+ years. Our release process includes beta testing, staged rollouts, and published schedules. Institutions are advised to install maintenance updates promptly and upgrade before EOL. For urgent issues, hot patches can be delivered to enterprise customers under SLA."

Nextcloud applies file integrity verification via MD5/SHA/PGP.

SURF has observed the following supporting documentation:
- Recent changelog showing the latest release within 20 days.
- Detailed release notes with component and security changes.
- Policy webpage describing patch process and advance patching for Enterprise customers.

A.6.1.5 Support (long term and incidents)

Nextcloud provides up to 5 years of support for older versions of the Enterprise software, for high and critical security issues (severity levels 2 and 1). These support terms also apply to

[152] Nextcloud reply to technical questions SURF, 18 July 2025.
[153] Idem.
[154] Nextcloud Enterprise Releases PDF, undated, https://cloud.nextcloud.com/s/kFyyoprCbTKJNA9?dir=/&editing=false&opendetails=true&openfile=true (last visited 16 February 2026)
[155] Nextcloud GitHub server maintenance and release schedule, page undated, URL: https://github.com/nextcloud/server/wiki/Maintenance-and-Release-Schedule (last visited seven February 2026).

the relevant client applications, as Nextcloud ensures availability of its official client applications in a version that is compatible with the maintained server version.[156]

Figure 32: Long term support for older versions (Enterprise Terms of Service)[157]

Year	Maintenance	Subscription level
1	All fixes and regressions across major versions released in the last 12 months.	Basic, Géant, Standard, Premium & Ultimate
2	Medium, high and critical security issues, data loss fixes, regressions within version	Premium, Ultimate
3 – 5	High and critical security issues, data loss fixes, regressions within version	Premium, Ultimate

Figure 33: Nextcloud severity levels for reported incidents[158]

Severity	Description
1	The issue is causing a total disruption of work, the product is inoperable and the issue is on a production environment.
2	The issue means that important features are inoperable on a production environment.
3	The product does not work as designed.
4	There is no loss of service. This may be a request for documentation or general information etc.

A.6.1.6 Secure coding

Nextcloud's code base is fully open source and publicly visible (published on GitHub). Nextcloud explained to SURF it has a review process which prevents or reduces risk of malicious code entry. In all, Nextcloud applies the following 5 measures to secure the code.

1. Review and approve all code changes by at least two core developers. As per Nextcloud, domain specific areas such as CalDAV require approval from designated code owners which is defined in their CODEOWNERS workflow.[159]
2. Nextcloud performs automated testing on all pull requests prior to merging. As per Nextcloud this includes unite and integration testing(PHP unit), front-end testing(Cypress and NPM), and performance testing across supported environments. [160]

[156] Nextcloud Enterprise Terms of Service, v3.8, last section of 'Long term support'.
[157] Screenshot from the Nextcloud Enterprise Terms of Service, v3.8.
[158] Idem.
[159] Nextcloud repository , code owners https://github.com/nextcloud/server/blob/master/.github/CODEOWNERS,last visited 16 April 2026.
[160] https://github.com/nextcloud/server/blob/master/.github/workflows/cypress.yml , https://github.com/nextcloud/server/pull/58436 and https://github.com/nextcloud/server/blob/master/.github/workflows/cypress.yml last visited 16 April 2026.

3. Nextcloud uses Psalm(an open source tool for PHP to detect errors, bugs and code quality) for static analysis on all relevant pull requests.[161] Additionally CodeQL is used to support security analysis of the codebase.[162] Nextcloud mentions that the DAST is not performed at their end, rather at the customer end.
4. Nextcloud describes that it follows secure coding practices based on OWASP guidelines.[163] Nextcloud also describes that secure coding guidance is provided through developer documentation and deployment security guidance applicable to the software.[164]
5. Nextcloud uses CodeQl and Psalm to detect insecure and potential hardcoded credentials. Nextcloud explained dependency management is handled using dependabot and Renovate with version pinning and cool down periods to mitigate supply chain attacks.[165]

With these measures Nextcloud follows SSDLC (Secure Software Development Life Cycle) practices. As per Nextcloud, security activities are integrated into the development process through code review, testing, static analysis and dependency management. The vendor also maintains secure coding guidelines on its website which are based on OWASP practices.[166]

A.6.1.7 Vulnerability management and CVE disclosure

Nextcloud publishes clear guidelines about the coordinated reporting of vulnerabilities.[167] Nextcloud also documents how it assists its customers with Common Vulnerabilities and Exposures (CVE). Nextcloud commits to specific timelines to disclose CVE after minor releases. The company also provides advance patches for special customers. This demonstrates a mature, risk-aware vulnerability management process. Nextcloud also maintains a public security advisory page linking to GitHub advisories. Each advisory details the vulnerability, references the pull request containing the fix, and shows the merged status. This demonstrates operational execution of vulnerability management and coordinated disclosure, providing evidence of the process in practice.

Nextcloud has a bug bounty program in place since 2016, in partnership with the HackerOne platform where security researchers can submit findings. The activity on the website shows resolved reports with payouts, indicating Nextcloud actively addresses issues reported through this channel. The platform has a responsible vulnerability disclosure policy, and appears to be actively maintained.[168]

Nextcloud refers to an external website with cve details. This only shows 1 vulnerability in 2024 and 1 in 2025, both scored medium.[169] SURF found another website named OpenCVE with several CVEs from 2025 , 2024 and before.[170] One of them is scored High. The issue is

[161] Psalm dev guide: https://psalm.dev/ last visited 16 April 2026.
[162] https://github.com/nextcloud/server/blob/master/psalm.xml last visited 16 April 2026.
[163]OWASP secure coding practices, URL: https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/stable-en/02-checklist/05-checklist (last visited 16 April 2026).
[164] Nextcloud security guidelines, URL: https://docs.nextcloud.com/server/latest/developer_manual/prologue/security.html.
[165] Nextcloud GitHub Dependabot, URL: https://github.com/nextcloud/server/blob/master/.github/dependabot.yml
[166] Nextcloud security guidelines, URL: https://docs.nextcloud.com/server/latest/developer_manual/prologue/security.html
[167] Nextcloud, Security, page undated, URL: https://nextcloud.com/security/ (last visited seven February 2026).
[168]Nextcloud Bug Bounty Program with HackerOne, URL: https://hackerone.com/nextcloud.
[169] CVE official website, undated, URL: https://www.cvedetails.com/vendor/15913/Nextcloud.html (last visited 8 February 2026)
[170] Open CVE website, undated, URL: https://app.opencve.io/cve/?q=vendor%3Anextcloud&page=2 (last visited 8 February 2026)

the ability to bypass 2FA.[171] Nextcloud also wrote that it publishes "*the exhaustive list of security advisories on GitHub and this is the Single Source of Truth.*[172]

A.6.1.8 Logging and auditing features

Nextcloud provides comprehensive logging and audit capabilities as tested for this DPIA. See Section A.3.3 in this DPIA, and the Technical Appendix. Admins can export or integrate the available audit logs in monitoring tools such as SIEM, DLP and MDM systems.

A.6.1.9 Software integrity and backdoor prevention

Nextcloud certifies in the amended DPA that it has not purposefully created any "backdoors" or similar programming in the Software that could be used by third parties to access the system and/or personal data. Nextcloud also commits in the DPA that it has not purposefully created or changed its business processes in a manner that facilitates such third-party access to personal data or relevant systems for Support and Update Services. Nextcloud finally certifies in the amended DPA with SURF there is no applicable law or government policy that requires Nextcloud to create or maintain back doors or to facilitate access to the Software or systems used for the Services. Although open-source software allows institutions to verify the integrity of the code and updates, institutions may not independently verify them in practice. As a result institutions continue to rely on Nextcloud's build and release processes. In theory, Nextcloud could push targeted updates without independent verification controls in place. Institutions hosting Nextcloud software themselves should therefore implement controls over what is deployed. They should also verify integrity, for instance by checking vendor signatures or hashes before installation and deploy updates only through controlled staging environments rather than directly into production. [173]

A.7 Parties and GDPR roles: processor and (joint) controller

The GDPR contains definitions of the different roles of parties involved in processing data: (joint) controller, processor and sub-processor.

Article 4(7) of the GDPR defines the (joint) controller as:
"*the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.*"

Article 26 of the GDPR stipulates that where two or more data controllers jointly determine the purposes and means of a processing, they are joint controllers. Joint controllers must determine their respective responsibilities for compliance with obligations under the GDPR in a transparent manner, especially towards data subjects, in an arrangement between them.

[171] Open CVE website example vulnerability scored High, undated, URL: https://app.opencve.io/cve/CVE-2024-37313 (last visited 8 February 2026)
[172] GitHub, URL: https://github.com/nextcloud/security-advisories/security/advisories. Reply Nextcloud to part A of this DPIA, 2 April 2026.
[173] NIST Special Publication 800-218, February 2022, PW.4.4, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf (last visited 19 May 2026)

Article 4(8) of the GDPR defines a processor as:
"*a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.*"

A sub-processor is a subcontractor engaged by a processor that assists in the processing of personal data on behalf of a data controller.

Article 28 GDPR sets out various obligations of processors towards the controllers for whom they process data. Article 28(3) GDPR contains specific obligations for the processor. Such obligations include only processing personal data in accordance with documented instructions from the data controller and cooperating with audits by a data controller. Article 28(4) GDPR stipulates that a data processor may use sub-processors to perform specific tasks for the data controller, but only with the prior authorisation of the data controller.

When data protection roles are assessed, the formal contractual division of roles is not leading nor decisive. The actual role of a party must primarily be determined on the basis of a **factual** analysis, rather than a **formal** analysis.

This section first assesses to what extent Nextcloud can currently be qualified as processor, based on the amended DPA with SURF. SURF and Nextcloud also agreed on a limitative list of further processing purposes, for which Nextcloud acts as authorised controller. This legal agreement prevents unintentional joint controllership, as addressed in Section A.7.4 below, or disclosure to Nextcloud as a third party. This construction will be explained in more detail in Section A.7.3 below.

A.7.1 The role of the Dutch education organisations

Education organisations are in control of most of the data processing because they manage the software themselves. The Dutch education organisations are an independent data controller for the data processing they permit through the configuration of the software, including for example, the use of third party apps. The education organisations are also in control of the personal data they collect and process in the different logs and in their first and second line support systems. They can *factually* exert a decisive influence on the purposes and means of specific processing activities, by enabling or disabling functionalities.

However, in order to be fully in control, the education organisations must also be able to determine the purposes of the (limited) processing by Nextcloud relating to admins and potentially other persons if such data are part of the third line support tickets or as part of user statistics. The organisations can only exercise such control if Nextcloud factually and formally acts as processor, and if the organisations are in control about any *further processing* purposes.

A.7.2 The role of Nextcloud as data processor

The EDPB emphasises in its guidance that the concepts of a controller and processor are functional concepts, based on a **factual rather than a formal analysis**. In most situations, the entity that qualifies as controller can be "*identified by reference to certain legal and/or factual circumstances from which "influence" normally can be inferred unless other*

elements indicate the contrary."[174] The legal circumstances mentioned by the EDPB are the presence of legal provisions requiring the controllers to collect and process some data. This is not relevant for the use of Nextcloud's self-hosted Enterprise software. However, Nextcloud does take decisions about the processing of the limited personal data it processes. The two subsections below provide a formal and factual analysis if Nextcloud can be qualified as data processor.

A.7.2.1 Formal analysis of processor role

As described in Section A.2.3 SURF and Nextcloud have agreed on a contract with an amended DPA for all SURF-members. As explained in Section A.5.2.1, the amended DPA contains an exhaustive list of 4 specific processing purposes. In abbreviated form:

1. Technically provide the software and applications via portal.nextcloud.com
2. Provide third level support
3. Help secure personal data processed by the customer in the software by sending update notifications and newsletters
4. Technically improve the software and services for all customers based on aggregated data.

Based on the technical analysis in Section A.3 and answers from Nextcloud about the factual data processing, SURF and Nextcloud have agreed to specify that the amended DPA covers 4 categories of personal data Nextcloud processes as processor:

1. Admin Account Data
2. The Diagnostic Data, both the optional data admins can share with Nextcloud GmbH, as well as logs generated by the company related to the use of the software
3. Support Data, including the metadata
4. Restricted Access Website Data (portal.nextcloud.com and support.nextcloud.com)

Processing is not limited to *storing*. As described in Section A.3 Nextcloud has taken technical measures to reduce or minimise the storage of personal data, but this section also addresses Nextcloud's role for the initial data collection.

Initially, Nextcloud incorrectly assumed the two types of Diagnostic Data it can collect (System Information Report and Usage Survey, plus information it collects via the Support App) were anonymous. However, Nextcloud has since agreed these data are pseudonymous personal data. Therefore the System Information Reports, Usage Survey Data and data Nextcloud collects via the support app, see Section A.3.3.2, as well as some of the logs described in Section A.3.3.3 that Nextcloud GmbH can generate (mainly via its sub-processors) are part of the newly defined processor tasks (other logs are part of the authorised further processing purposes, see Section A.7.3 below).

[174] EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.1, Adopted on 07 July 2021, par. 21, URL: https://edpb.europa.eu/system/files/2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf.

The relevant 6 processor logs[175] are:

1. Visits to the restricted access Support Hub website (part of Website Data)
2. Log of outbound email to admins including security newsletters (via ActiveCampaign / Postmark)
3. Software download and update log
4. Push notification proxy log
5. Activity log in Zammad's support ticketing system
6. Log of privacy / access requests (via DataCo) for processor data

For Nextcloud to be able to provide secure, well-functioning, bug free and up to date software, the processing of some personal data (including admin contact data to send security updates, Diagnostic Data, both in its own logs and in the System Information Reports and Usage Survey data, as well as personal data shared via support requests) about the configuration and use of the software may be necessary. In order to achieve such clear objectives, the data processor has a certain liberty to decide how the personal data are processed and in which systems (with which means). However, the processor must be transparent about what personal data it needs to process, and for what purposes, in order to successfully claim to act on instructions of the controller. Because this data processing is now covered by the amended DPA with SURF, the education organisations/controllers are formally in control that Nextcloud only processes personal data when necessary for specific and legitimate purposes. Based on the amended DPA Nextcloud *formally* qualifies as data processor for the tested software and services, and as authorised controller for the further processing of some processor data for Nextcloud's own specific legitimate business purposes. See Section A.7.3 below.

By agreeing to a limitative list of specific purposes, SURF and Nextcloud have also agreed that descriptions in Nextcloud's Privacy and Legal Policy relating to the personal data cannot apply to the education organisations covered by the amended SURF DPA. Additionally, SURF and Nextcloud have included three specific processing prohibitions:

1. Nextcloud shall not process Personal Data for any "further" or "compatible" purposes (within the meaning of Articles 5(1)(b) and 6(4) GDPR) other than those specified in this DPA or enabled by the Customer account administrator.
2. Nextcloud will not Process Personal Data for advertising purposes or serve advertising in the software and services and Nextcloud will not process Personal Data for direct marketing, profiling, research or analytics purposes except where such processing is necessary to comply with Customer's Instructions (commercial mailings to procurement officers, if the customer has not opted-out).
3. Nextcloud will not Process Personal Data for content scanning or monitoring purposes, including scanning for Child Sexual Abuse Material ("**CSAM**").

In sum, based on the new DPA with SURF, Nextcloud can *formally* act as processor for the agreed purposes (both as processor, and as controller for the authorised further processing purposes).

[175] The 7th log mentioned in Section A.3.3.3 is part of the authorised legitimate business purposes.

A.7.2.2 Factual analysis of processor role

This section uses four relevant criteria to assess if Nextcloud **factually acts as data processor**, and not only formally, based on the amended DPA with SURF. These four criteria are:

1. The engagement of sub-processors.
2. The right to audit.
3. Determination of data retention periods of the Account, Diagnostic, Support and Website Data.
4. Decisions about data subjects' rights

Engagement of sub-processors

For the risk assessment in this DPIA it is relevant whether customers have meaningful control over the engagement of sub-processors by Nextcloud and the processing of their personal data by such sub-processors.

As data controllers, the education organisations must be able to authorise Nextcloud's sub-processors (via SURF's centrally negotiated DPA). As processor, Nextcloud must impose the same data protection obligations on its sub-processors as those imposed to itself by SURF. Legally, sub-processors can benefit from the docking clause in the amended DPA, that the agreement from Nextcloud with the education organisation also applies to sub-processors.

Table 5: Nextcloud table in the amended DPA with all potential sub-processors

Name of Subprocessor	Data transferred	Location of storage	Purpose of Processing	Duration	Locations of access[176]
Zammad GmbH	Name, email address, support tickets	Germany	Provider of the Nextcloud support portal	Same as subscription	
AC PM, LLC	Email content	United States – Adequacy decision (certified under the EU-US Data Privacy Framework)	E-Mail Delivery Service (Postmark)	Same as subscription	
Collabora Ltd	Company name, name, email address number of licenses, duration of contract, support data	United Kingdom	Provision of licenses and support Services for Nextcloud Office	Same as subscription	
Hetzner Online GmbH	Name, email address	Germany	Hosting of portal.nextcloud.com	Same as subscription	

[176] Nextcloud will publish the locations of access on nextcloud.com by end of Q3 2026.

Odoo SA	Name, email address (commercial and admin)	Belgium	Provision of security information and updates	Same as subscription	
OpenProject GmbH	Company name, name, email address number of licenses, duration of contract, support data	Germany	Provision of licenses and support Services for OpenProject	Same as subscription	
Open-Xchange AG	Company name, name, email address number of licenses, duration of contract, support data	Germany	Provision of licenses and support Services for Dovecot Pro	Same as subscription	
Sendent BV	Company name, name, email address number of licenses, duration of contract, support data	Netherlands	Provision of licenses and support Services for MS Outlook Add-in, MS Exchange Connector, MS Teams Integration	Same as subscription	
Struktur AG	Company name, name, email address number of licenses, duration of contract, support data	Germany	Provision of licenses and support Services for the Nextcloud Talk High Performance Back-end and SIP bridge	Same as subscription	
Stalwart Labs Ltd.	Company name, name, email address number of licenses, duration of contract, support data	United Kingdom	Provision of licenses and support Services for Stalwart	Same as subscription	
Thinkfree Inc.	Company name, name, email address number of licenses, duration of contract, support data	South Korea	Provision of licenses and support Services for Thinkfree Office	Same as subscription	
XWiki SAS	Company name, name, email address number of licenses, duration of contract, support data	France	Provision of licenses and support Services for XWiki	Same as subscription	

The list of relevant (sub) processors in scope of this DPIA is:

- Collabora Ltd (DPA based on SCC controller-processor, dated 17 October 2025)
- Zammad GmbH (DPA dated 15 July 2021)
- Struktur AG (DPA based on SCC controller-processor, dated 24 July 2025) (not tested)
- DataCo GmbH (DataGuard) (DPA dated July 2025, only for the DSAR form)
- AC PM, LLC for Postmark mailings (DPA dated 3 May 2022)

In the amended DPA with SURF Nextcloud commits to only engage subprocessors that process personal data in the EU, with two temporary exceptions.

These two exceptions are:

1. the use of mailing services by a provider in the USA (Admin Account Data and Commercial Contact Data), until Q3 2026. Nextcloud is actively searching for an EU based mail provider.
2. access by UK based employees of Collabora to relevant support tickets in Zammad (if the customer chooses this Office software). The data transfer to the UK is based on the adequacy decision from the European Commission. If that decision becomes invalid, Nextcloud will limit access to EU-based employees.

The amended DPA with SURF also ensures Nextcloud gives the education organisations 60 business days advance notice (except in emergency situations) before the engagement of new sub-processors.[177] The amended DPA specifies:

"*Nextcloud shall notify Customer of the intended engagement of a new subprocessor (including the name and location of the relevant subprocessor, and the activities it will perform and a description of the Personal Data it will process) at least sixty (60) business days before the new subprocessor starts processing any Personal Data. To enable such notifications, Customer shall subscribe to the respective mailing list via portal.nextcloud.com.*"

The organisations have 15 business days to object upon receipt of the notice. This period should give universities or other large education organisations sufficient time to be able to effectively object to such changes prior to the engagement of the concerned sub-processor(s). The amended DPA prevents Nextcloud from simply ceasing to provide services in case the customer objects. If reply to an objection, Nextcloud will either cancel the plan to use the new subprocessor, take steps to remove the cause for the objection, or cease to provide a service that involves the new subprocessor, but in that case, provide the customer with commercially reasonable alternatives.

The use of cookies can also involve third parties. However, the technical analysis of cookies on the customer-hosted server, and cookies set and read by Nextcloud itself on the

[177] Nextcloud DPA template, Section 7.7, Use of Sub-processors.

restricted access support portal (and admin sign-in portal) shows that Nextcloud by default only sets and reads first party cookies.

In view of the effective right to object and the agreed limitations to the data transfers, Dutch education organisations are in control over this data processing.

Right to audit
The amended DPA includes the right for SURF to conduct an audit on behalf of the Dutch education organisations, to verify Nextcloud's compliance with the provisions of the DPA for the processing of personal data. SURF can invoked this right once a year, except in respect of an additional audit following (i) a Nextcloud data breach or (ii) if specifically ordered by Customer's national Supervisory Authority.

The right to audit is an important guarantee for SURF that it can verify the effective data processing, and hence, can support the education organisations factually exercise their role as data controllers and comply with their obligation in Art. 5(2) of the GDPR to provide evidence of their (processor's) compliance with the principles of the GDPR.

Determination of retention periods
Determining how long data are stored, is also a decision that can only be taken by a data controller. Deciding how long data are available, is a decision about the *means* of the processing. As will be elaborated in Section A.11 Nextcloud has provided adequate documentation to SURF about the retention periods of the Account Data, Diagnostic Data, Support and Website Data that Nextcloud collects. This means Dutch education organisations are able to demonstrate compliance with the principle of transparency about the data processing.

As described in Section A.3.4 SURF and Nextcloud have agreed on a reduced retention period of 15 months for closed support tickets (instead of the default 4 years). Though Nextcloud does not offer a Do It Yourself option to admins to delete tickets or attachments, admins can ask Nextcloud to delete individual tickets and attachments prior to the 15 months retention period, via a support request. Additionally, in reply to this DPIA Nextcloud introduced a warning to admins on portal.nextcloud.com, when they attach files, to not upload sensitive personal data. Nextcloud has agreed with Zammad to implement the same warning on support.nextcloud.com in Q3 2026.

Together these mitigating measures enable the education organisations/controllers to be factually in control of the retention period of the Support Data.

Decisions about data subjects' rights
As described in Section A.3.6, Nextcloud has agreed to provide a complete reply to a DSAR request from an admin, both in its role as processor, and its role as authorised controller (to the extent an individual can be identified as many of the authorised further processing purposes only involve aggregated data). This includes access to any collected Usage Survey Data, historical logs about the use of the Support Portal, frozen webserver access logs - provided Nextcloud can reliably verify the identity of the data subject, and the activity logs kept by Postmark (or future EU based mail service provider).

A.7.3 Role of Nextcloud as authorised data controller (legitimate business purposes)

Nextcloud necessarily has to process some personal data for its own legitimate business operations. To prevent unintentional joint controllership, Nextcloud has agreed to include a limitative list of authorised further processing purposes in the DPA, as quoted in Section A.5.2.1.

In abbreviated form the seven purposes are:

1. Comply with legal obligations
2. Billing, fulfilling of orders and receiving payments
3. Customer relationship management
4. Licensing compliance/fraud detection
5. Use statistical data for internal reporting, financial reporting and product strategy
6. Create (restricted access) website analytics
7. Use statistical data to technically improve and optimise the performance and efficiency of the software

With regard to potential **requests for disclosure from government authorities**, Dutch education organisations only allow Nextcloud to process the limited personal data it has access to as independent data controller in the following circumstances:

- Nextcloud will reject any order from authorities outside of the EEA.
- If the order comes from an authority in the EAA, Nextcloud will first conduct a thorough legal review, and attempt to redirect to the Enterprise customer if it is a valid order.
- Where possible and legally viable, Nextcloud shall judicially object to the request or order or the prohibition to inform the Controller about this request or order.
- Nextcloud will only provide the minimum necessary data and refuse to make any changes to the software that will create backdoors to the customer instance.
- Nextcloud will inform its customer as soon as legally permitted
- Nextcloud will publish annual transparency statistics relating to the number of disclosure requests it has received, and how many it has complied with.

The agreement on the (limits to the) processing of the **license data for fraud detection** offers an important protection for end users. It follows from the Terms and Conditions that organisations must keep records of the license data, and Nextcloud grants itself the right to conduct an in-situ inspection of the raw (end user) license data to verify the organisation's compliance. This opens a formal legal way for Nextcloud to obtain access to personal data from end users it would normally never have access to. In reply to this observation Nextcloud added: "*An in-situ inspection could give Nextcloud incidental access to end user license data it otherwise never processes. However, the amended DPA limits this processing to what is strictly necessary and proportionate for the agreed licensing compliance purpose.*"[178]

[178] Nextcloud reply to company confidentiality input request, 7 July 2026.

As described in the box with mitigating measures at the end of Section A.3.2 Nextcloud has agreed to clearly distinguish in the portal between **Commercial Contacts and admins**. This should prevent confusion about Nextcloud's role as processor for the admin contact data, and Nextcloud's role as authorised controller for the Commercial Contact Data. By Q3 2026 the different employees with their different roles can decide themselves to what mailing lists they wish to subscribe to or unsubscribe from (commercial, security updates, updates about new subprocessors).

As authorised controller, Nextcloud will comply with the clauses in the amended DPA relating to privacy by design and default on its public website, confidentiality, security, Processing exclusive to the European Economic Area ("EEA") and the right to audit for SURF. Not all of the provisions in the DPA apply to Nextcloud in its role as authorised controller. Most importantly, the legitimate engagement of processors (not sub-processors) is Nextcloud's own responsibility under the GDPR. In that role, Nextcloud uses the services from the New Zealand based cloud analytics provider Matomo, and hence transfers personal data out of the EU (but only if the visitors agree to 'analytic' cookies). Nextcloud is similarly free to directly report data breaches to its commercial contacts. Nextcloud has explained it is difficult to distinguish in its CRM between prospective customers and Commercial Contact Data.

A.7.4 Nextcloud as independent controller

As mentioned in Section A.5.2.3 Nextcloud describes many processing purposes as independent data controller in its public legal documentation. Of course, Nextcloud has the liberty to process some personal data for its own legitimate business purposes. But there is no such liberty when the collection of personal data is the result of the data controller's decision to engage a company's software and services as data processor. As processor, Nextcloud may not *further* process the personal data it collects and generates as a result of the engagement of its software and support services by an Enterprise customer for its own purposes. If a processor exceeds the boundaries of its role, by processing personal data for purposes not authorised by the data controller, based on Art. 28(10) of the GDPR, it factually acts as a data controller. However, not as an independent data controller. If the data processing for the processor's own purposes is inextricably linked to the collection of these data in a role as processor, the processor has to be qualified as joint controller with the customer that enables the processing by using this provider.

Nextcloud can still process some personal data as independent data controller, as long as it concerns personal data that are not related to the use of the Enterprise software and services. If Nextcloud processes personal data based on consent from end users, such as when users voluntarily attend Nextcloud events, participate in Nextcloud's public forum or consent to advertising cookies, there is no risk of role confusion. As long as such data processing is completely optional, teachers and students can freely give valid consent. Nextcloud is an independent data controller for the data processing via its public website, but Nextcloud has committed in the amended DPA to maintain the current privacy friendly default cookie settings, that is, only set analytic and social media cookies with the freely given consent of the visitor.

As a result of the clarification of the purposes and the role of Nextcloud as processor or authorised controller in the amended DPA with SURF, there is no longer a risk of unintentional joint controllership. As described in Section A.7.2.2, based on this amended DPA with SURF, education organisations can exercise effective control over the sub-processors, retention periods and exercise of data subjects' rights. By agreeing on a limitative list of authorised legitimate business purposes with Nextcloud, the education organisations can effectively fulfil their obligations as (independent) data controllers.

A.8 Interests in the data processing

A.8.1 Interests of SURF/education organisations

SURF and the education organisations have a strategic and ethical interest in investing in EU sovereign solutions. Wladimir Mufty, SURF's program manager for digital sovereignty, explains in a blog what SURF means with digital sovereignty: "*we mean having control, influence, direction, freedom of choice, and the necessary innovative strength within an increasingly digital world.*"[179]

Mufty explains how SURF and Kennisnet have operationalised the application of the 3 core values autonomy, humanity and justice in a 'value compass', and writes that digital sovereignty is necessary, it's a condition, to uphold and protect values such as privacy, autonomy and inclusion.[180]

SURF and the education organisations have a strong ethical interest in protecting the personal data processed from and about employees, students, and all individuals whose personal data can be processed by the Office software, not only against the risk of potential unauthorised disclosure to foreign (notably US American) governments, but also against the risk of unavailability of personal data, due to potential sanctions or other types of pressure that may stop cloud providers from providing services.

SURF has a cultural and security compliance interest in promoting the use of open source software. Mufty explains: "*It helps safeguard public values such as efficiency, transparency, autonomy, and privacy. Think of the use of open standards, the ability to customize software yourself (or by your commercial IT partner/provider), and better control over security and compliance. It aligns with principles we as a sector feel at home with, as we have for decades in open science, open access, open standards, or open educational resources.*"[181]

SURF has a business continuity interest in preventing dependencies on suppliers, both relating to 'legacy' software and to vendor lock-in. The SURF vendor compliance team has invested in multiple umbrella DPIAs and security assessments, and in a contracting system that helps the education organisations choose between multiple compliant suppliers. To prevent vendor lock-in, education organisations need to have the organisational and technical ability to easily transfer their data to other suppliers over time. Because Nextcloud is built on open standards, the exportability is almost built-in.

[179] SURF blog Wladimir Mufty, Digital sovereignty, autonomy, and public values: what exactly do we mean? 11 July 2025, URL: https://communities.surf.nl/en/publieke-waarden/article/digital-sovereignty-autonomy-and-public-values-what-exactly-do-we-mean
[180] Idem.
[181] Idem.

Many Dutch education organisations use services from Microsoft for text and number processing. From a security interest it makes sense for organisations to choose a different provider, also in view of the risk that Microsoft is likely to attract more threats due to its near monopoly for Office services. The Dutch government Audit Office has explicitly warned the Dutch government about this risk.[182] The near monopoly is not unique for the Netherlands, but a global problem. The concentration results in a very large collection of confidential data that gives state actors an important motive for developing attack capabilities on M365.[183]

A.8.2 Interests of Nextcloud

Nextcloud has a short mission statement: "*We develop software for decentralized and federated clouds as alternative to centralized cloud services.*"[184]

Nextcloud has a key business interest in positioning itself on the Enterprise and Education market as the only serious European alternative for the US American dominance of Microsoft and Google. Nextcloud stresses data sovereignty as a key reason to adopt its products.

"*The best solution for governments is to be digitally sovereign, or in other words, have control over your digital destiny. Nextcloud offers governments the most ideal package – a self-hosted, private cloud solution that's under your full control. No data escaping to third parties, no vendor lock-in, a fully auditable code and lastly, industry leading security and collaboration features.*"[185]

Nextcloud announced on 5 November 2025 that it will invest over 250 million euro in digital sovereignty from 2026-2030.[186] CEO Frank Karlitschek was quoted saying:

"*Since the beginning of the year, interest in Nextcloud has tripled. Potential customers are also stating very clearly that they see dependency on big tech as a risk. We demonstrate that sovereign alternatives to big tech are not only possible, but already available.*"[187]

On 17 December 2025 Nextcloud also announced expanding its Dutch ecosystem, including a partnership with KPN to offer the software as a managed cloud service.[188]

As a result of the dramatically changed relationship with the USA, many Dutch and European organisations are reconsidering their decisions to entrust personal data to a global cloud service provider. By providing open source software, Nextcloud has a business development interest in claiming that all data processing exclusively takes place in the EU and to emphasise that this control precludes the need to move data at a future date based on court or political decisions.

[182] Auditdienst Rijk, Onderzoeksrapport Bevindingen onderzoeksopdracht 'Evaluatie public cloudbeleid Rijksoverheid', 3 July 2024, URL: https://www.tweedekamer.nl/downloads/document?id=2024D38837
[183] Idem, p. 5.
[184] Nextcloud, Our principles, 12 August 2019, URL: https://nextcloud.com/blog/the-nextcloud-mission-and-principles/ .
[185] Nextcloud blog, Nine Nextcloud features for government users, 24 May 2023, URL: https://nextcloud.com/blog/9-nextcloud-features-for-government-users/
[186] Nextcloud blog, Sovereignty 2030: Nextcloud invests over €250 million in digital sovereignty, 5 November 2025, URL: https://nextcloud.com/blog/press_releases/nextcloud-invests-in-digital-sovereignty/ .
[187] Idem.
[188] Nextcloud, Powering digital sovereignty in the Netherlands: Nextcloud expands Dutch ecosystem, 17 December 2025, URL: https://nextcloud.com/blog/powering-digital-sovereignty-in-the-netherlands-nextcloud-expands-dutch-ecosystem/ .

Nextcloud writes:

"*With on-premises hosting and strong encryption features, Nextcloud allows businesses to maintain compliance with EU privacy laws while avoiding the risks associated with US-based services*"[189]

However, Nextcloud is not yet 100% EU based, since Nextcloud does engage one US American processor (Postmark) to send mail to customers, uses Matomo in New Zealand for website statistics and does rely on the US American owned GitHub and Hugging Face repositories for customers to download the software and AI models, and for developers to contribute and participate in the open source community. Moreover, in reply to this DPIA Nextcloud has confirmed GitHub is the single source of truth for security advisories (See Section A.6.1.7) These dependencies mean that Nextcloud Enterprise can not yet attain the highest score in the new European Commission Cloud Sovereignty Framework.[190]

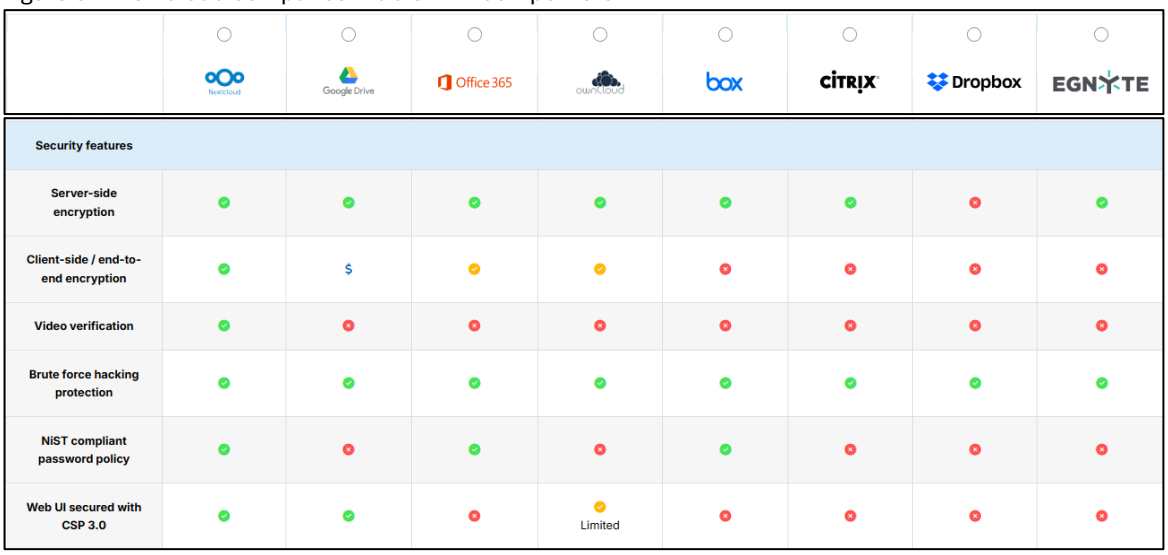
In reply to this observation, Nextcloud wrote:

"*GitHub is widely regarded as the industry standard for open source software development. Switching to a European platform would mean not only the migration effort, but also losing a significant portion of the global contributor community. We are keeping an eye on other platforms, not limited to the EU/EEA, and periodically review the costs and benefits of switching. No switch is planned at this time, but awareness of the issue exists.*"[191]

Like its competitors, Nextcloud has strong business ethical interests to comply with international privacy and security standards. Nextcloud sells itself, in a comparison with other providers as '*best in security, largest ecosystem and easiest to use*'.[192] Nextcloud explains it has a USD 10.000 security bug bounty program, "[which] *brings top security expertise in, keeping your data safe*."[193]

[189] Nextcloud, EU-US Data Privacy Framework is defunct: what does this mean for businesses?, 23 April 2025, URL: https://nextcloud.com/blog/eu-us-data-privacy-framework-is-defunct-what-does-this-mean-for-businesses/
[190] European Commission, Cloud Sovereignty Framework, version 1.2.1, October 2025, URL: https://commission.europa.eu/document/download/09579818-64a6-4dd5-9577-446ab6219113_en
[191] Nextcloud reply to part A of this DPIA, 2 April 2026.
[192] Nextcloud, What makes Nextcloud the best choice, undated, URL: https://nextcloud.com/compare/ (last visited 18 February 2026).
[193] Idem.

Figure 34: Nextcloud comparison table with competitors[194]



	Nextcloud	Google Drive	Office 365	ownCloud	box	CITRIX	Dropbox	EGNYTE
Security features								
Server-side encryption	✓	✓	✓	✓	✓	✓	✗	✓
Client-side / end-to-end encryption	✓	$	✓	✓	✗	✗	✗	✗
Video verification	✓	✗	✗	✗	✗	✗	✗	✗
Brute force hacking protection	✓	✓	✓	✓	✓	✓	✓	✓
NiST compliant password policy	✓	✗	✓	✗	✓	✗	✗	✗
Web UI secured with CSP 3.0	✓	✓	✗	✓ Limited	✗	✗	✗	✗

A.8.3 Joint interests

The interests of Nextcloud and SURF align when it comes to strategical issues of sovereignty and autonomy. The two hyperscalers that offer the most frequently Office productivity suites are based in the USA, and their use always involves international data transfers to data centres and engineers in third countries. Nextcloud's status as a German company, and the absence of a systematic data flow from the self hosted Enterprise software and client applications to Nextcloud aligns well with current geopolitical risks.

SURF and Nextcloud also have a joint interest in an objective assessment of the level of sovereignty. The European Commission has defined Sovereignty Effectiveness Assurance Levels in its Cloud Sovereignty Framework.[195] Nextcloud plans to end its current dependency on a US American mail provider soon, in Q3 2026. However, the use of the two US American software repositories prevents Nextcloud from attaining a high score, and does not align with SURF's interest in preventing data transfers out of the EU.

The interests of Nextcloud and the Dutch education organisations may align with regard to the interest in strong security, but may also conflict. As part of the shared security interest, the availability of many audit logs and configurability of those logs serves an important security requirement for the organisations as data controllers. However, the deployment of open source software also puts a burden on organisations: they have to find and train IT admins that can keep the software up to date, secure and well functioning, and they have to have internal support staff for the first and second line. Many education organisations have reorganised their internal IT support and outsourced many tasks to cloud suppliers. If enough education organisations show an interest in the use of Nextcloud Enterprise, SURF may step in as intermediary, and develop a new Nextcloud hosted service for its members.

[194] Idem, last visited 14 May 2026.
[195] European Commission, Cloud Sovereignty Framework, version 1.2.1, October 2025, URL: https://commission.europa.eu/document/download/09579818-64a6-4dd5-9577-446ab6219113_en

With regard to security, as assessed in Section A.6, SURF and Nextcloud have a mutual interest in the external validation of Nextcloud's security with a CSPN certification, and the confirmation that Nextcloud has fixed al medium and high risks found by the code security review by the German BSI.

A.9 Processing Locations

The education organisations are largely in control over the processing locations: they decide where they host the Enterprise software. They can host themselves, or involve a partner organisation in the Netherlands such as KPN, or a German partner like IONOS.[196]

Analysis of the potential transfer of personal data outside of the EU is therefore limited to transfers to, and by (sub) processors.

The GDPR contains specific rules for the transfer of personal data to (sub) processors or controllers in third countries without an adequate level of protection. The adequacy can be determined in a number of ways: a multinational may adopt Binding Corporate Rules, apply the EU Standard Contractual Clauses (SCC) or only transfer to countries for which the European Commission has taken a so-called adequacy decision (such as the USA since June 2023, or New Zealand, or the UK).

Based on the amended new DPA with SURF Nextcloud GmbH as processor does not transfer the limited personal data it processes (mostly Support Data) out of the EU. However, Nextcloud can have sub-processors, such as Collabora, outside of the EU. In that case, Nextcloud primarily relies on adequacy decisions, but may also rely on SCC's for transfers to these (optional) sub-processors, the EU Standard Contractual Clauses (controller to processor, as revised in 2021). The SCCs contractually ensure a high level of protection. However, they are not by themselves sufficient for data transfer to a country without an adequate level of data protection.

A.9.1 Transfers via (sub) processors

As described in Section A.7.2.2 Nextcloud factually transfers personal data to a (sub)processor in the USA. Nextcloud uses **Postmark** (the company ActiveCampaign LLC) for delivery of all of its outbound mails. As evidenced with a mail header example in the Technical Appendix, the outbound traffic includes, but is not limited to, the newsletters Nextcloud sends to admins and Commercial Contacts.

The data transfer via Postmark is based on the adequacy decision for the USA, as well as the use of Standard Contractual Clauses (SCC). ActiveCampaign is certified under the Data Privacy Framework program for EU-US data transfers.[197]

Admins cannot realistically unsubscribe from these mails without risking missing essential security warnings. In reply to this observation Nextcloud has committed to switch to a different EU based provider in Q3 2026.[198]

[196] Nextcloud, A sovereign Microsoft 365 alternative: Nextcloud and IONOS join forces, 25 June 2025, URL: https://nextcloud.com/blog/nextcloud-workspace-microsoft-365-alternative-by-nextcloud-and-ionos/
[197] ActiveCampaign LLC, active registration for non-HR data under the EU US DPF, URL: https://www.dataprivacyframework.gov/list
[198] Nextcloud reply 6 May 2026 to questions SURF 17 April 2026.

Nextcloud also uses the US American repositories from **GitHub** and **Hugging Face** to distribute its software and share essential information about common issues, fixed issues and releases. These parties are independent controllers and third parties for Nextcloud and for the education organisations. The transfer is based on the EU US adequacy decision. GitHub is registered as participant to the EU US Data Privacy Framework, Hugging Face is not.[199]

Nextcloud also describes in its Privacy and Legal Policy that it uses **Matomo** cloud services for website analytics on its public website. This data transfer is only relevant if visitors decide to consent to analytic cookies: by default Nextcloud only sets functional cookies.

Matomo Cloud is provided by InnoCraft Limited, a company based in New Zealand. Like the USA, New Zealand benefits from a European Commission decision that it has an adequate level of data protection. This means no additional safeguards are necessary for this data transfer.

Though Matomo explains that its customers can choose to have "*100% of your data and backups securely stored in Europe, our company is based in New Zealand and we have contracts with AC3 NZ and they're in contract with AWS New Zealand.*"[200]

Nextcloud describes that it has configured Matomo to anonymise the IP addresses from its website visitors.

"*Our website uses Matomo with the "AnonymiseIP" extension. This ensures that IP addresses are processed in abbreviated form, i.e. anonymised, maintaining user anonymity during web analysis. The IP address transmitted by your browser via Matomo is not merged with other data collected by us and is not transmitted to third parties.*"

Matomo itself describes that it collects the following personal data (prior to anonymisation[201]):

"***Customer Instance Usage Data -*** *when you use the Matomo Cloud service, we monitor the instance activity relating to that Customer ID (e.g., time of first login into the app and first tracking requests, features visited, number of Users logged in; number of hits, goals, funnels, users, websites and segments configured and active (to manage quota allowances for each Customer account); number of events created or tracked per day (adding new User, website, or a plugin); conversion from trialist to full account; support request event trigger). We process this usage data for statistical purposes, to improve Matomo Cloud services and to recognise and stop any misuse of the Customer Account.*"[202]

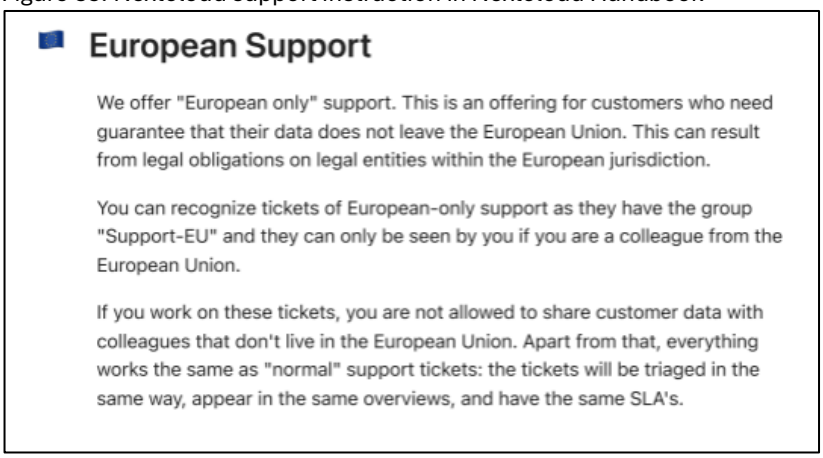
Matomo also explains that its customers must inform their website visitors that this is processing of personal data. "*Although the IP address is anonymised immediately, the*

[199] https://www.dataprivacyframework.gov/list 'GitHub', page last visited 14 May 2026.
[200] Matomo, In which locations does the Matomo Cloud store the data?, undated, URL: https://matomo.org/faq/in-which-locations-does-the-matomo-cloud-store-the-data/ (last visited 18 February 2026).
[201] Matomo, How does IP address anonymisation work, undated, URL: https://matomo.org/faq/general/how-does-ip-address-anonymisation-work-in-matomo/
[202] Matomo Cloud Privacy Policy, effective date 9 October 2025, URL: https://matomo.org/matomo-cloud-privacy-policy/

initial collection and processing of personal data (before anonymisation) still falls under data protection laws."[203]

With regard to the third line support, the German company **Zammad** hosts its support ticketing system and web interface in Germany. However, Nextcloud tells employees via the internal Nextcloud Handbook that they can only access support data from EU Enterprise customers if they are physically located in the EU. This implies that Nextcloud does have support employees located outside of the EU but also that Nextcloud has taken measures to prevent data transfer through geographical access restriction. SURF could not find documentation about this separation, but Nextcloud explained that the separation is working on a technical level due to the creation of groups with different access rights.[204]

Figure 35: Nextcloud support instruction in Nextcloud Handbook[205]



Per request of SURF Nextcloud has ensured that access for employees of Collabora to the relevant support tickets in Zammad is limited to employees physically located in the EU and the UK. Nextcloud has also committed to limit the access to EU based employees if the adequacy decision for the UK becomes invalid.

Mitigating measures Nextcloud:

- Nextcloud will change to an EU-based mail delivery provider in Q3 2026.
- Nextcloud has limited the access to Collabora support tickets in Zammad to Collabora employees physically located in the EU and the UK.
- Nextcloud will restrict access to the Collabora tickets to employees physically located in the EU if the adequacy decision for the UK becomes invalid.

[203] Matomo, What to include in a GDPR-compliant Privacy Notice, undated, URL: https://matomo.org/faq/how-to/how-to-write-a-gdpr-compliant-privacy-notice/ (last visited 18 February 2026).
[204] Nextcloud reply to part A of this DPIA, 2 April 2026. Nextcloud referred to information from Zammad at https://admin-docs.zammad.org/en/6.2/manage/groups/access-levels.html
[205] Nextcloud shared a screenshot about European Support from the Nextcloud Handbook, not publicly available.

A.9.2 Data Transfer Impact Assessment

As long as the adequacy decisions for the USA (or New Zealand and the UK) are not annulled, Dutch education organisations can rely on the EU US DPF and adequacy decisions, or alternatively, on the SCCs Nextcloud has in place for transfers outside of the EU, **without having to take extra data protection measures**.

However, Nextcloud itself writes that it doubts the factual validity of the adequacy decision in a blog about legal developments in the USA.[206] Therefore Nextcloud explains it has also concluded SCC with Postmark.

Formally, if Nextcloud is convinced the USA cannot effectively offer adequate data protection, it should have also performed a Data Transfer Impact Assessment (DTIA) to assess the probability and impact of a disclosure order from a US government authority to Nextcloud's (sub) processors in the USA (Postmark), New Zealand (Matomo) and the UK (Collabora). The DTIA would have to list extra technical and organisational measures to lower the probability of occurrence of the risk of unauthorised disclosure.

To help education organisations assess the probability of compelled disclosure, Nextcloud has agreed to publish annual government requests transparency reports. Nextcloud told SURF it has never received a request for disclosure, and does not expect any government is interested in the limited personal data it processes.[207]

A.10 Legal and Policy Framework

This section only describes the additional obligations arising from the current ePrivacy Directive. This section does not discuss the ePrivacy Regulation, proposed by the European Commission in 2017.[208] After a protracted trialogue between the European Commission, the European Parliament and the European Council, it became obvious that no consensus could be reached. In March 2025 the European Commission formally withdrew the proposal. This means Nextcloud will have to comply with the current (Dutch and European) ePrivacy rules.

In view of the limited scope of this DPIA, other legal obligations or frameworks are not included in this report. This section describes two relevant ePrivacy obligations: related to cookies, and related to commercial mailings.

The act of reading or placing information (through cookies or similar technology), or enabling third parties to read information from the devices of end users triggers the applicability of Article 5(3) of the ePrivacy Directive, regardless of who places or reads the information, and regardless of whether the content is personal data or not. Consent is required prior to the retrieval or storage of information on the devices or browsers of end users, unless one of the exceptions applies, such as the necessity to deliver a requested service, or necessity for the technical transmission of information.

[206] Nextcloud, EU-US Data Privacy Framework is defunct: what does this mean for businesses? 23 April 2025, URL: https://nextcloud.com/de/blog/eu-us-data-privacy-framework-is-defunct-what-does-this-mean-for-businesses/
[207] Nextcloud reply to part A of this DPIA, 2 April 2026.
[208] European Commission, Proposal for a Regulation on Privacy and Electronic Communications, 10.1.2017 COM(2017) 10 final, URL: https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation

Based on article 3(1) of the GDPR, because the data processing takes place in the context of the activities of data controllers (Dutch education organisations), the GDPR applies to all phases of the processing of these data.

Applicability of the GDPR rules does not exclude applicability of the ePrivacy rules or vice versa.

The EDPB writes:

"Case law of the Court of Justice of the European Union (CJEU) confirms that it is possible for processing to fall within the material scope of both the ePrivacy Directive and the GDPR at the same time. In Wirtschaftsakademie, the CJEU applied Directive 95/46/EC notwithstanding the fact that the underlying processing also involved processing operations falling into the material scope of the ePrivacy Directive. In the pending Fashion ID case, the Advocate General expressed the view that both set of rules may be applicable in a case involving social plug-ins and cookies."[209]

Article 5(3) of the ePrivacy Directive was transposed in article 11.7a of the Dutch Telecommuni-cations Act. The consequences of the so-called cookie provision are far-reaching, since it requires clear and complete information to be provided **prior** to the data processing, and it requires consent from the user, unless one of the legal exceptions applies. The consent is identical to the consent defined in the GDPR.

The ePrivacy rules apply to four types of data processing related to cookies by Nextcloud,:

- Cookies and similar technology on the public website
- Cookies and similar technology on the restricted access Support Portal
- Cookies and similar technology on the self-hosted Nextcloud server software
- The use of a tracking pixel in the newsletters

Privacy Company did not observe any Telemetry Data sent to Nextcloud or any third-party domains from the web or client applications.

Nextcloud uses a cookie consent banner on its public website. Sometimes admins and legal staff have to visit Nextcloud's publicly accessible website, to look up essential technical and legal information. As analysed in Section A.3.5.1 Nextcloud's documentation about these cookies was inaccurate. Even if a visitor refused all but the essential cookies, Nextcloud was observed to set and read two cookies from the category of 'Convenience cookies', even though Nextcloud writes these cookies are only set with consent. As verified by SURF, Nextcloud has fixed this problem on 29 April 2026.

Nextcloud applies privacy by default on its admin and support portals. There is no consent banner, but Nextcloud only sets and reads first party functional cookies. Nextcloud

[209] EDPB, Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, adopted on 12 March 2019, Paragraph 30. URL: https://edpb.europa.eu/sites/edpb/files/files/file1/201905_ edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf In footnotes the EDPB refers to: CJEU, C-210/16, 5 June 2018, C-210/16, ECLI:EU:C:2018:388. See in particular paragraphs 33-34 and the Opinion of Advocate General Bobek in Fashion ID, C-40/17, 19 December 2018, ECLI:EU:C:2018:1039. See in particular paragraphs 111-115.

currently does not document these cookies, but has committed to update the information in July 2026.

The Nextcloud software itself also sets cookies, but does not show a consent banner to the end user when visiting the self hosted Nextcloud instance. As shown in the box with mitigating measures at the end of Section 0 Nextcloud has improved the documentation for admins about the cookies in the self-hosted software with information about

- The exact names of the cookies it sets.
- The purposes of the cookies with sufficient granularity.
- The retention period or expiry date of the cookies, and the difference between those, where the retention period is determined by Nextcloud in the software.

Nextcloud does not document it uses a tracking pixel in its newsletters. Nextcloud uses the open source software suite Odoo to create emails. This software automatically includes a tracking pixel in every outgoing mail. See the details in the Technical Appendix.

Via Odoo Nextcloud collects interaction data, such as reading, opening or clicking on the newsletters from Nextcloud (see Section A.3.3.3). Postmark explains it can log these interactions for webmails with the help of invisible 1x1 pixels.[210] Nextcloud does not inform potential or actual subscribers about this reading of information from their devices/browser. Following earlier advice from WP29[211], the EDPB has also explained the use of tracking pixels falls in the scope of Article 5(3) of the ePrivacy Directive.[212]

The EDPB explains: "*In the case of an email, the sender may include a tracking pixel to detect when the receiver reads the email. Tracking pixels on websites may link to an entity collecting many such requests and thus being able to track users' behaviour.*"[213] and "*The addition of tracking information to URLs or images (pixels) sent to the user constitutes an instruction to the terminal equipment to send back the targeted information (the specified identifier) (...) As a consequence, it can be considered that the collection of identifiers provided through such tracking mechanisms constitutes a 'gaining of access' in the meaning of Article 5(3) ePD, thus it applies to that step as well.*"[214]

Nextcloud could theoretically use these data to create profiles of reading behaviour of recipients. Such processing is prohibited based on the amended DPA with SURF for the newsletters addressed to admins and commercial contacts, but SURF has no control over the processing by Nextcloud as independent data controller, when Nextcloud for example subscribes people that have downloaded whitepapers or attended events to its commercial newsletter.

[210] ActiveCampaign, Postmark, How does open tracking work?, last updated 14 March 2025, URL: https://postmarkapp.com/support/article/782-how-does-open-tracking-work.
[211] Article 29 Working Party, WP29 Opinion 9/2014, p. 9, URL: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp224_en.pdf .
[212] EDPB, Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive, adopted seven October 2024, URL: https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202302_technical_scope_art_53_eprivacydirective_v2_en_0.pdf .
[213] Idem, p. 13, par 48.
[214] Idem, p. 13 par. 51.

Because the information about the reading behaviour can be used for profiling purposes, and does not meet the requirements of necessity, Nextcloud should ask for consent for the use of the tracking pixel. Nextcloud can make the data collection via the tracking pixel lawful in two ways:

1. if Nextcloud informs recipients and asks for consent or
2. if Nextcloud informs recipients and finds a way to immediately and irretrievably aggregate the usage data in RAM memory of Odoo to ensure Nextcloud has no technical way to correlate behaviour of a specific recipient to these logs. In that case Nextcloud can possibly argue under the Dutch Telecommunications Act that it has taken appropriate measure to prevent infringements on the fundamental rights, and in analogy with a 6(1) f reasoning, claim a legitimate interest.

Additionally, as discussed in Section A.3.2, Nextcloud did not distinguish between admins and commercial contacts (procurement officers). The contact provided by a customer was automatically subscribed to a company newsletter with a commercial purpose. The legal grounds for unsolicited commercial mailings are governed by Article 11.7 of the Dutch Telecommunications Act. Generally, informed consent is required, except when the recipient has provided the contact data in the context of the sales of a product or service, and the recipient was able to object in an easy way and free of costs against the use of the electronic contact data for that purpose.

Nextcloud does offer an opt-out option at the bottom of each newsletter, but did not provide the required ex ante information to the commercial contacts.

Mitigating measures Nextcloud:

- Nextcloud has disabled the tracking pixel in Odoo, and will investigate the option for immediate aggregation.
- In the self-service Nextcloud portal (portal.nextcloud.com) customers will be able in Q3 2026 to distinguish between admin and commercial contacts and decide themselves to subscribe and unsubscribe to commercial and technical newsletters.
- Nextcloud will update the information about cookies on the restricted access websites in July 2026.

A.11 Retention Periods

This section describes the retention periods the education organisations themselves can determine, and the retention periods determined by Nextcloud, in a factual role as controller.

A.11.1 Retention periods determined by the education organisations

Nextcloud explained to SURF how it helps admins control the retention periods of Accounts and of Files. [215]

[215] Nextcloud answers to technical questions SURF, 18 July 2025.

Nextcloud provides two apps for retention purposed:

- account_retention to disable and then remove unused accounts[216]
- files_retention to delete data past a certain duration.[217]

Figure 1: Default Account retention periods

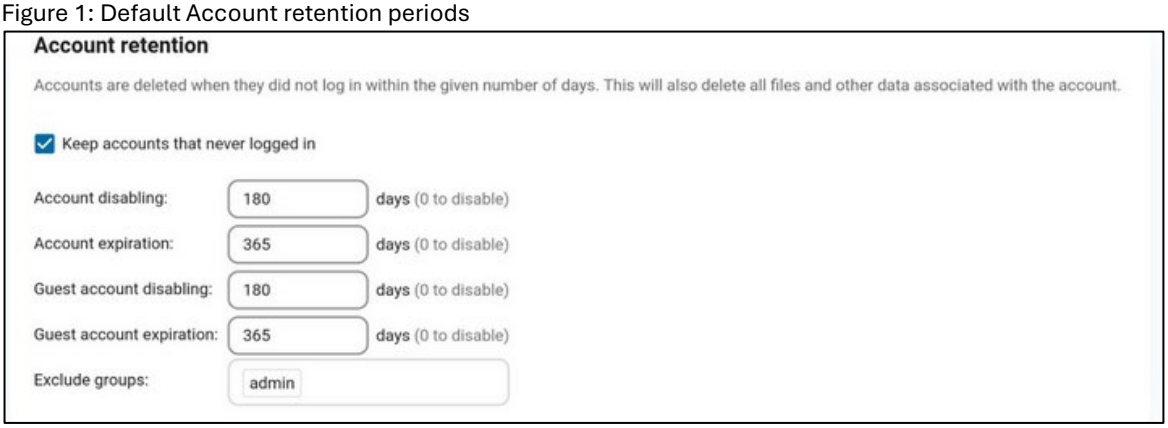
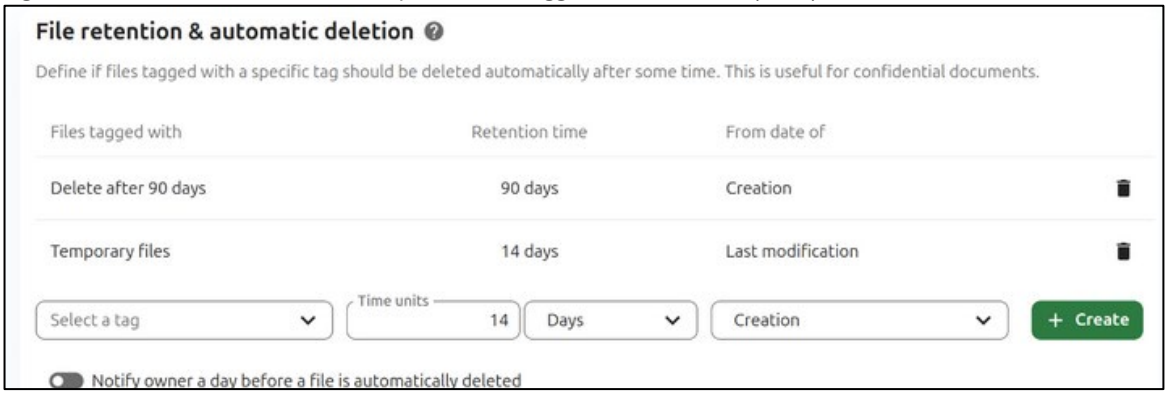


Figure 2: Default automatic deletion periods for tagged Content Data (Files)



Nextcloud also offers a central control to admins to change the automatic retention period of 28 days for chats, after which the chat will be automatically erased. There is no such control for channels in Talk. Nextcloud explained that this intentional: "*certain Talk rooms can be kept forever. However, inside a chat, moderators can define the expiration period for chat messages.*"[218]

Table 6: Predefined retention periods in the Nextcloud software

Data category	Retention period
Account Data	Admin determines individual or automatic deletion after period of inactivity (default 180 days)
Content Data	If files are tagged, admins can decide on automatic deletion. The default period is 90 days after creation, and 14 days for temporary files.

[216] Nextcloud App store, Account Retention, last updated: 3 weeks ago, URL: https://apps.nextcloud.com/apps/user_retention (last visited 18 February 2026).
[217] Nextcloud, Retention, undated, URL: https://apps.nextcloud.com/apps/files_retention (last visited 18 February 2026).
[218] Nextcloud reply to part A of this DPIA, 2 April 2026.

Support Data	As long as the organisation decides (in its own support ticketing system for 1st and 2nd line support)
Diagnostic Data (audit logs managed by admin audit app)	Login attempts: no period but size limit, default up to 100 MB, after which a new logfile can be created or the existing one overwritten.
	File access by users: no period but size limit, default up to 100 MB.
	Automatic deletion tasks: no period but size limit, default up to 100 MB.
	Talk interaction logs: managed by admin

A.11.2 Retention periods Nextcloud as processor

In its internal Data Protection Handbook, Nextcloud explains it applies data minimisation and storage limitation.

***"Data minimisation** - the core aspect of data minimisation refers to the principle of necessity. According to this principle, all processing activities must be designed in a way that personal data is processed only when necessary to achieve the specific purpose. These principles play a decisive role, for example, when defining internal retention periods.*

***Storage limitation** - storing personal data on a "just in case" basis is not allowed. Personal data should only be stored for as long as it is necessary for the respective processing purpose."*

The amended DPA with SURF contains a list with specified retention periods for the agreed processor purposes for the four relevant categories of personal data: the admin account data, the (optional) Diagnostic Data, Support Data (including metadata) and the restricted access Website Data.

Nextcloud by default retains the support ticket and the metadata for four years after the issue has been solved, in its role as processor. Commonly, a period of 13-15 months suffices for most customers. As described in the box with mitigating measures at the end of Section A.3.4 Nextcloud has agreed on two mitigating measures. Customers can ask Nextcloud to delete specific tickets and attachments, or all tickets before a certain date and Nextcloud has reduced the retention period for SURF-members to 15 months after closure of the support tickets.

Nextcloud uses the support ticketing system from its sub-processor Zammad. Zammad retains the separate activity log (as described in Section A.3.3.3) for 42 days.

Nextcloud stores the webserver access logs for seven days. If a visitor accepts analytical cookies (disabled by default), Nextcloud uses Matomo to create website analytics. Matomo removes the last two octets of the IP address of visitors.

Table 7: Retention periods Nextcloud processor

Data category	Retention period
Admin Account Data	Subscription to security update newsletter: until consent is withdrawn.
	(Postmark) Email log with metadata and content: 45 days.
Support data	Support tickets 13-15 months after ticket closure.
	Support system activity log: 42 days
Diagnostic data	Usage Survey: one (1) year
	System Information Report: accessible for Nextcloud for two (2) weeks after an admin has shared the link.
	Configuration data and user stats collected via Support App: as long as the contract exists.
	Sending of update push notifications: Until the app is deinstalled or the account removed from the device (Nextcloud only stores the date, device ID and use of its public key).
Website Data	Visits to the restricted access Support website and the admin portal: max seven days
	Cookie storage in application logs: none. There is a maximum 'expiry date' of 30 days for (some) cookies in the end user browser according to Nextcloud's Privacy and Legal Policy
All data	Log of privacy / access requests (via DataCo): two (2) years after the request

A.11.3 Retention periods Nextcloud as authorised controller

The amended DPA with SURF also includes a specification of the different retention periods when Nextcloud processes personal data for its legitimate business purposes, as authorised controller. See Table 8 below.

Incidentally Nextcloud can retain support tickets for seven tot 10 years if the support ticket documents a contractual dispute, where a customer asks for reimbursement or damages via a support ticket, and/or engages in legal procedures against Nextcloud. In that case, Nextcloud is authorised to *further process* these specific Support Data as controller, to the extent strictly necessary for Nextcloud's legitimate business purposes. Nextcloud confirmed that it does not qualify all support tickets as business correspondence or accounting or tax relevant information, as defined in § 257 HGB and § 147 AO, only in exceptional cases. In such an exceptional case Nextcloud will inform the customer it will exceptionally retain the support tickets about a specific topic for that necessary longer period.

Table 8: Retention periods Nextcloud as data controller

Data category	Retention period
Commercial Contact Data	*"for as long as necessary for the respective purposes. After that, we delete it unless we are permitted or required to retain it longer (due to statutory retention obligations or for the establishment, exercise or defence of legal claims"*[219] Nextcloud mentions several different purposes, amounting to a retention period of 10 years: • Preparation, conclusion and execution of contracts: for the duration of the business relationship, plus two years for documentation and evidence purposes. • Communication within the business relationship (including email, phone, etc.): deleted after two years. Only in exceptional cases, if the communication forms part of contractual or evidentiary documentation, the statutory retention periods apply (up to 10 years). • Fulfilment of legal obligations (e.g., commercial and tax law retention obligations): the contract up to 10 years. • Enforcement of legal claims and defence in legal disputes: retained until final clarification, additionally within applicable limitation periods, generally 3 years.
	Subscription to company newsletter: until consent is withdrawn.
Support Data	Aggregated support tickets and metadata: necessity decided by Nextcloud
	In incidental cases, 7-10 years, for compliance with statutory retention periods under the German Fiscal Code (AO) and German Commercial Code (HGB). This is only the case if a support ticket documents a contractual dispute, where a customer asks for reimbursement or damages via a support ticket, and engages in legal procedures against Nextcloud.
Diagnostic Data	License distribution (via a partner like Sendent): As long as necessary to fulfil the contract.
	log about outbound email with Commercial Contact Data (via Postmark): 45 days
	Aggregated data: not personal data

[219] Nextcloud Privacy and Legal Policy, Section XIV. Processing of Personal Data of Customers, Prospects and Suppliers.

Part B Assessment of Lawfulness of Data Processing

This second part of the DPIA assesses the lawfulness of the data processing. This part contains a discussion of the legal grounds, an assessment of the necessity and proportionality of the processing, and of the compatibility of the processing in relation to the purposes.

B.1 Legal grounds

To be permissible under the GDPR, processing of personal data must be based on one of the grounds mentioned in Article (6) (1) GDPR. Essentially, for processing to be lawful, this article demands that the data controller bases the processing on the consent of the user, or on a legally defined necessity to process the personal data.

The assessment of available legal grounds (sometimes called 'lawful bases') is tied closely to the principle of purpose limitation. The EDPB notes that

"*The identification of the appropriate lawful basis is tied to principles of fairness and purpose limitation*. [...] *When controllers set out to identify the appropriate legal basis in line with the fairness principle, this will be difficult to achieve if they have not first clearly identified the purposes of processing, or if processing personal data goes beyond what is necessary for the specified purposes.*"[220]

Thus, in order to determine whether a legal ground is available for a specific processing operation, it is necessary to determine for what purpose (s), the data was or is collected and will be (further) processed. There must be a legal ground for each of these purposes. The appropriate legal ground depends on Nextcloud's GDPR role. As analysed in Section A.7 based on the amended DPA with SURF, Nextcloud formally and factually qualifies a processor, but is permitted to *further* process some (generally aggregated) data for its own legitimate business purposes. In that second role, Nextcloud qualifies as authorised controller.

As described in Section A.3, Nextcloud processes limited personal data relating to the use of the self-hosted Enterprise software, in 4 categories:

1. Account Data (admin Account Data and Commercial Contact Data).
2. Diagnostic Data (Usage Survey, System Information Report, data collected via the Support app and the seven logs the company generates itself).
3. Support Data (including metadata).
4. Website Data (both the restricted access websites portal.nextcloud.com and support.nextcloud.com).[221]

The sections below discuss the appropriate legal ground for each category of personal data from the perspective of the Dutch higher education organisation.

[220] EDPB, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects - version adopted after public consultation, 16 October 2019, URL: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_en .
[221] As explained in Section A.7.4, Nextcloud is an independent data controller for the public website, but has committed to maintain privacy by default settings.

Table 9: Types of personal data processing in relation to Nextcloud's role

Category of personal data	**Nextcloud as processor**	**Nextcloud as authorised controller**
Admin Account Data	Send update notifications and newsletters	Comply with legal obligations
Commercial Contact Data	-	Send newsletters
		Billing, fulfilling of orders and receiving payments
		Customer relationship management
		Comply with legal obligations
End user licenses	-	Use statistics about the number of users to verify licensing compliance: possibly verify with an in-situ audit
		Use statistical data for internal reporting, financial reporting and product strategy
Diagnostic Data	Use aggregated Diagnostic Data to technically improve the software and services for all customers, including bug fixing, troubleshooting, patching, and general maintenance.	• Comply with legal obligations • Use statistical data for internal reporting, financial reporting and product strategy • Use statistical data to technically improve and optimise the performance and efficiency of the software
Support Data	Provide third level support/technical assistance based on 3d line requests from customers	
	Use aggregated Support Data to technically improve the software and services for all customers, including bug fixing, troubleshooting, patching, and general maintenance	
Website Data	Technically provide the software and applications via portal.nextcloud.com and support.nextcloud.com.	Website analytics (with consent)

In Section B.2 below, only the potentially valid legal grounds for education organisations will be discussed. The legal grounds of legal obligation (Article 6 (1) (c) GDPR) and of vital interest (Article 6 (1) (d) GDPR) are not discussed, since nor Nextcloud (as processor) nor education organisations have a legal obligation or a vital (lifesaving) interest in processing personal data via Nextcloud Enterprise (even though SURF acknowledges Nextcloud may be required to process limited personal data following legal obligations).

The last subsection B.2.4 discusses the compatibility of the authorised further processing of the limited personal data by Nextcloud.

B.2 Legal grounds for education organisations

B.2.1 Consent

Article 6 (1) (a) GDPR reads: *"**the data subject has given consent** to the processing of his or her personal data for one or more specific purposes"*

Education organisations generally cannot rely on consent from employees (admins and procurement officers). In view of the imbalance of power between employees and employers, consent can seldom be given freely. Employees must be free to refuse or withdraw consent for the processing of their personal data without facing adverse consequences

Additionally, public sector organisations should refrain from relying on consent for the processing. In the context of Recital 43 of the GDPR, the EDPB explains:

"whenever the controller is a public authority, there is often a clear imbalance of power in the relationship between the controller and the data subject. It is also clear in most cases that the data subject will have no realistic alternatives to accepting the processing (terms) of this controller. The EDPB considers that there are other lawful bases that are, in principle, more appropriate to the activity of public authorities."[222]

There are three circumstances in which Nextcloud asks for consent:

1. Use of cookies that are not strictly necessary
2. Sending of commercial and technical newsletters
3. Collection of Diagnostic Data (via the Usage Survey, System Information Report and via the Support app)

Nextcloud asks visitors of its publicly accessible nextcloud.com website for consent for other than strictly functional cookies and asks admins and procurement officers for consent when they sign up for a newsletter. As described in Section A.10 Nextcloud by default only sets strictly functional cookies on its restricted and publicly accessible websites, and has improved the cookie documentation (but not for the functional cookies on the admin and support portal).

Nextcloud has also committed to distinguish between admins and commercial contact data, and will allow them by Q3 2026 to separately and voluntarily subscribe to the different newsletters. Nextcloud has also stopped using the invisible tracking pixel to track user interactions such as opening and clicking. Nextcloud incorrectly did not inform its different categories of recipients, and did not ask for consent for the reading of this information with an invisible tracking pixel. In view of the legal requirement from the ePrivacy Directive to ask for consent for non-necessary cookies (and similar information read from the end user device), Nextcloud could not rely on other legal grounds for this processing either.

Nextcloud has also taken mitigating measures to ensure that admins can give informed consent when they share the Usage Survey data. As described in Section A.3.3.2 Nextcloud

[222] EDPB, *Guidelines on consent*, paragraph 3.1.1.

now offers admins an equal choice between 'Yes' and 'No', and no longer sends a monthly reminder to admins to enable sharing of the Usage Survey Data.

To adequately document the context of support requests, admins can generate and share the System Information Report with Nextcloud. If they use Nextcloud's official support app, they can create the System Information Report in a web interface, and provide valid consent when they decide to share these data (provided they are authorised by their organisation to share these data). But if they use the support app, the app also periodically sends some user statistics and information about installed apps to Nextcloud, without a consent request or other visibility. See Section A.3.3.2.3. Therefore this data flow cannot be based on consent.

B.2.2 Necessary for the performance of a contract

Article 6 (1) (b) GDPR reads: "*processing is **necessary for the performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.*"

As described in A.5.1, Dutch education organisations can use the tested core Nextcloud Enterprise applications for many specific purposes. Generally speaking, organisations will use productivity software for 4 general purposes:

1. Facilitate (international) collaboration, information sharing and communication between employees and students in- and outside of the education organisation, including guest users.
2. Reduce commuting/enable hybrid working.
3. Provide first and second line support to employees and students.
4. Use reports and logs for purposes such as maintenance, installing updates, troubleshooting, bug fixing and data breach detection/solution, in line with the organisation's internal IT policy.

To be able to successfully invoke the legal ground of 'performance of a contract' for the use of Nextcloud Enterprise with respect to end users, the processing of the personal data via Nextcloud Enterprise has to be strictly necessary for the performance of the contract with each individual data subject. It makes sense for an education organisation to require all employees to work with the same software suite, in this case Nextcloud Enterprise, to be able to maintain central data access boundaries and create a single source for data storage. If they do make use of Nextcloud Enterprise mandatory, they can also rely on this legal ground for the 3d and 4th general purpose, to use the available logs in the self-hosted software to provide support, and to keep the software secure and up to date.

It is less plausible that use of Nextcloud Enterprise would be strictly necessary for students in order to perform their study tasks. Students generally maintain their own laptops, and are free to choose other productivity software as long as they can complete required tasks in the prescribed formats. This legal ground of necessity for the performance of a contract is not available for other recipients or data subjects whose data may be processed in or with the Nextcloud software, as the education organisations do not have a contract with these people.

B.2.3 Necessary for a task in the public or a legitimate interest

Article 6 (1) (e) GDPR reads: *"processing is necessary for the performance of a **task carried out in the public interest** or in the exercise of official authority vested in the controller"*.

Article 6 (1) (f) GDPR reads: *"processing is **necessary for the purposes of the legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child***.**

Public sector organisations are excluded from relying on legitimate interest when processing personal data for public services. The last sentence of Article 6 (1) of the GDPR explains: *"Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks."* This excludes the application of the legitimate interest ground for processing carried out by public sector organisations in the performance of their tasks.
However, the choice to use Nextcloud Enterprise will usually be secondary to the performance of public tasks by Education organisations and can therefore be considered as a task primarily exercised under private law, for which the legitimate interest of the organisation can be a valid legal ground for processing.

The legal ground of necessity for a legitimate interest as defined in Article 6(1) f of the GDPR can for example be used in relation to necessary functional and analytical cookies. This follows from the specific Dutch legislative history. As described in Section 10, there is a specific exception in the Dutch Telecommunications Act on the consent-requirement for 'innocent' analytical cookies, that is for cookies with no, or relatively small impact on the private life of website visitors.[223] To determine this impact, the Dutch legislator has explicitly referred to the elements of the legitimate interest test in Article 6(1) f of the GDPR (at the time, the similar test in Article 8(f) of the Data Protection Directive).

Both legal grounds (public interest and legitimate interest) require an assessment of the necessity of the personal data processing, of the proportionality and availability of alternative, less infringing means to achieve the same legitimate purposes (subsidiarity). It is up to the different education organisations (and their privacy officers) to determine what legal ground is best suited for specific processing purposes.

As mentioned in the analysis of consent above, Nextcloud has programmed the support app to periodically share data about installed apps and number of users. Organisations can prevent this data flow by instructing admins not to use the support app, but generate system information reports via the console. However, if Nextcloud adequately documents this data sharing, not only as part of this DPIA, it is plausible that organisations can rely on the necessity for their legitimate interest for this processing.

B.2.4 Compatibility of authorised further processing

As analysed in Section A.7.3, SURF and Nextcloud have agreed on a list of authorised *further* processing purposes in the amended DPA. This means Nextcloud is allowed to process some of the personal data it obtains in a role as processor for some other specific

[223] Kamerstukken II 2013/14, 33902 (Wijziging van de Telecommunicatiewet (wijziging artikel 11.7a)), nr. 3 (Memorie van Toelichting).

purposes. SURF has assessed the compatibility of these processing purposes with the original processor purposes.

In abbreviated form the seven authorised further processing purposes are:

1. Comply with legal obligations
2. Billing, fulfilling of orders and receiving payments
3. Customer relationship management
4. Licensing compliance/fraud detection
5. Use statistical data for internal reporting, financial reporting and product strategy
6. (restricted access) Website analytics
7. Use statistical data to technically improve and optimise the performance and efficiency of the software

Without such an agreement on authorised further processing, Nextcloud would not be allowed to process the personal data for these useful and legitimate purposes, not as processor and not as controller. Processors are not allowed to make decisions about the purposes and means of processing. A processor that would make such decisions, would violate the GDPR and become an independent controller, based on Article 28 (10) of the GDPR.

Article 28 (10) GDPR reads: "*Without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.*"

As unauthorised data controller (without joint controller agreement or agreement about further processing) Nextcloud would qualify as a third party for these processing activities. Education organisations generally do not have a legal ground for bulk disclosure of personal data from employees and students to third parties.

To assess the legitimacy of further processing for a different purpose, following Article 6 (4) of the GDPR, SURF has taken (at least) the following 5 criteria into account:

a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;
d) the possible consequences of the intended further processing for data subjects;
e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Under a (**link**), the use of aggregated data for the agreed legitimate business purposes, including forecasting and improving the efficiency of the website and (support) services, aligns with the education sector's interest in well-functioning and up to date Enterprise software. The processing of the Commercial Contact Data plus payment and license information for invoicing and customer relationship management is inevitable for maintaining a future-proof financially healthy supplier. Only the first purpose, of

compliance with legal obligations, stands out. Education organisations have to accept that Nextcloud as a company has to comply with legal obligations under German or EU law.

Under b (**relationship**), Nextcloud is formally authorised to process the aggregated data and the commercial data as data controller. By giving this instruction the Dutch education organisations formally take the decision about the (compatibility of the) purposes of the processing, and remain in control. As with the assessment above of the *link*, the fact that Nextcloud has to comply with legal obligations under German or EU law is a legal fait accompli, even though there is no relationship with the purposes for which the education organisations procure the Nextcloud Enterprise software. The Commercial Contact Data include personal data from the people in education organisations that perform procurement and vendor relationship management tasks. These employees have a logical expectation that suppliers will process their contact data.

Under c (**nature**) Nextcloud GmbH collects limited personal data relating to the use of the Nextcloud Enterprise software. Content Data are only processed in the Enterprise software as installed by the customer (on premises or as a managed service by a Nextcloud partner), and cannot be accessed by Nextcloud GmbH. However, the support tickets and attachments can include data of a sensitive or confidential nature, but Nextcloud has implemented safeguards (see the section under e below). The Diagnostic Data collected or generated by Nextcloud only include limited pseudonymous information, no information relating to Content Data such as file names or URLs.

Under d (**consequences**), the authorised further processing may result in loss of control and loss of confidentiality of sensitive Admin Account Data and Support Data, in combination with security sensitive information about configuration choices made by admins, especially if Nextcloud were to be compelled by a non-EU authority to disclose these personal data, or forced to create a backdoor in a specific update shipped to a specific education organisation. As long as Nextcloud still uses a US American company for email services, and relies on two US American platforms (GitHub and Hugging Face) for downloads of its software and information about security critical updates, these companies may be compelled to disclose personal data to US American authorities. Such disclosure can have a medium to high impact on admins, if they become the target of spear phishing by state actors.

Under e (**safeguards**) as authorised data controller Nextcloud can only process (pseudonymised) personal data when strictly necessary and proportionate for the agreed legitimate business interests. With regard to the first purpose, of compliance with legal obligations, SURF and Nextcloud have agreed on a clear set of rules. See the explanation about legal obligations in Section A.5.2.2. If Nextcloud receives an order for compelled disclosure of personal data from an non-EU authority, it will unconditionally reject. Only if Nextcloud receives such an order from an EU-authority, it can comply, but only after having first verified the validity, attempted to redirect to the proper controller, the education organisation, and contesting the order where legally viable. When complying, Nextcloud will only disclose the minimum required data, and Nextcloud will publish annual reports how often it has received requests, and how often it has actually complied. As an extra assurance that Nextcloud GmbH cannot be compelled to disclose Content Data to government authorities, in or outside of the EU, SURF and Nextcloud have agreed on a no backdoor policy. See Section A.6.1.9.

The amended DPA with SURF also explicitly prohibits Nextcloud from taking any decisions about further processing for other purposes. As highlighted in Section A.5.2.1, Nextcloud may not take any decision about further processing for other purposes, or from processing for advertising, marketing, profiling, research or analytics purposes, unless the customer explicitly instructs Nextcloud to process for such purposes.

To ensure the compatibility of the further processing of the Support Data, Nextcloud and SURF have agreed on 5 extra safeguards for the Support Data, as shown in the box with mitigating measures at the end of Section A.3.4:

- Nextcloud has added a warning for admins on portal.nextcloud.com not to upload any personal data in attachments.
- Nextcloud has agreed with Zammad to implement the same warning on support.nextcloud.com in Q3 2026.
- Since 10 May 2026, only Collabora employees physically located in the UK and the EU can access the relevant tickets in Zammad, not any employees located in other countries outside of the EU
- In case the adequacy decision for the UK is no longer valid, Nextcloud will ensure that only EU based employees of Collabora can access the support tickets.
- Nextcloud has reduced the retention period of closed support tickets for SURF-members to 15 months. Additionally, customers can ask Nextcloud to remove specific or all support tickets and attachments before a certain date.

In sum, based on the amended DPA and the agreed mitigating measures Nextcloud's further processing of the limited Account, Commercial Contact, Diagnostic, Support and Website Data for the agreed seven purposes is compatible with the purposes for which Nextcloud receives and generates data as a processor.

B.3 Special Categories of Data

Special categories of data are "*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, data concerning a natural person's sex life or sexual orientation*" (Art. 9(1) GDPR).

Additionally, based on Article 10 GDPR, the processing of personal data relating to criminal convictions and offences or related security measures is similarly restricted.

As explained in Section 2.2 of this DPIA, the variety of personal data that organisations can process with Nextcloud Enterprise cannot be overestimated. Nextcloud does not have access to any Content Data, including special categories of data, processed by the education organisations in the Nextcloud Enterprise software.

It is up to the individual education organisation as data controllers to assess what special categories of data they process in the contents of Talk conversations, Groupware mailboxes and calendars, or documents stored in Files. It is up to the organisations to ensure only authorised workers have access to special categories of data with the group based access controls (see Section A.6.1.3).

The (third line) support tickets and attachments Nextcloud can collect can include data of a sensitive or confidential nature. Nextcloud has added a warning for admins on portal.nextcloud.com not to upload any personal data in attachments and Nextcloud has agreed with Zammad to implement the same warning on support.nextcloud.com in Q3 2026. It is up to the individual education organisation as data controllers to assess what special categories of data they (are allowed to) process in the support data.

B.4 Purpose Limitation

The GDPR obliges data controllers to comply with the principle of 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), not be considered to be incompatible with the initial purposes*" (Article 5 (1) (b) GDPR).

Essentially, the above means that the controller must have a specified purpose for which he collects personal data and can only process these data for purposes compatible with that original purpose, unless the controller can meet additional requirements before any further processing can take place.

Data controllers must be able to prove based on Article 5(2) of the GDPR that they comply with this purpose limitation principle (accountability). Data controllers cannot comply if they engage a supplier as a data processor, but ignore that that provider also reserves the contractual right to process (some) personal data for its own purposes, in its own commercial business interest. As described in Section A.5.2.3 Nextcloud mentions many processing purposes as independent controller in its Legal and Privacy Policy plus Terms and Conditions. But as analysed in Section A.7.4 Nextcloud can only legitimately qualify as independent (not unintentional joint) controller for the following purposes: processing of the public website data (limited to functional cookies), offer access to a public Nextcloud forum and comply with legal (content removal) obligations for this forum, process copyright complaints via the abuse mail address, communicate via social media, organise events, and recruit and select employees.

To prevent independent decisions from Nextcloud on the processing of personal data (as joint controller or as a third party) for the remaining purposes, the improved DPA with SURF contains two limitative lists of processor and authorised further processing purposes. As assessed in Section B.2 processing for the agreed specific 4 processor purposes is necessary for the execution of the contract with admins, respectively fulfilment of a legitimate interest or public task. As assessed in Section B.2.4 Nextcloud's further processing of specific personal data, generally aggregated, for the agreed specific further processing purposes, is compatible with the agreed data collection purposes.

The principle of purpose limitation is closely linked to transparency and 'fairness' of the processing. Together, implementation of these principles should lead to surprise

minimisation for the education organisations. As the Article 29 Working Party wrote in its guidelines on transparency (adopted by the EDPB):

"A central consideration of the principle of transparency outlined in these provisions is that the data subject should be able to determine in advance what the scope and consequences of the processing entails and that they should not be taken by surprise at a later point about the ways in which their personal data have been used. This is also an important aspect of the principle of fairness under Article 5.1 of the GDPR and indeed is linked to Recital 39 which states that "[n]atural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data(...)."[224]

Since most of the data processing takes place in the self-hosted software, the primary burden of transparency lays on the education organisations as data controllers. They must inform employees and students for what specific purposes they will process personal data, as part of the Content Data, and as part of the 1st and 2nd line support, as well as in the different Diagnostic Data logs.

Additionally, they must inform admins and the procurement officers in the organisation about the agreed purposes for which they permit Nextcloud to process the (limited) personal data. Both of these lists of purposes (and exclusions of invasive purposes) can be added to an internal data processing policy.

Finally, as part of surprise minimisation, education organisations must inform other persons whose personal data may be processed in the Nextcloud software as part of the Content Data about the purposes of the processing. These purposes can be added to an existing publicly accessible data protection policy.

Dutch education organisations that want to use the Nextcloud Enterprise software can use this DPIA and the amended DPA to update their register of processing activities and inform the relevant employees accordingly.

SURF is able to verify Nextcloud's compliance with the agreed purposes based on the extensive audit right in the amended DPA. Based on the new agreement with SURF, and the right to audit, education organisations are able to comply with Article 5(2) of the GDPR, and prove they comply with the principle of purpose limitation (accountability).

In sum, based on the amended DPA with the agreed limitative lists of agreed purposes, and agreement on key terms such as anonymisation, Nextcloud's (limited) data processing is in line with the requirement of purpose limitation, both as processor and as authorised data controller.

B.5 Necessity and Proportionality

Article 5(1)c GDPR requires that every processing has to be limited to what is necessary to achieve the set purpose(s). It is therefore important to examine whether every processing is in fact necessary for the purposes for which the data controllers process personal data.

[224] The EDPB has adopted the Article 29 Working Party guidelines WP 260 rev 1, Guidelines on transparency under Regulation 2016/679, adopted on 29 November 2017, as last Revised and Adopted on 11 April 2018, Par. 41.

The concept of necessity is made up of two related concepts, namely proportionality and subsidiarity. The personal data which are processed must be necessary for the purpose pursued by the processing activity. First, it has to be assessed whether the same purpose can reasonably be achieved with other, less invasive means. If so, these alternatives have to be used.

Second, proportionality demands a balancing act between the interests of the data subject and the data controller. Proportionate data processing means that the amount of data processed is not excessive in relation to the purpose of the processing. If the purpose can be achieved by processing fewer personal data, then the amount of personal data processed should be decreased to what is necessary. Therefore, essentially, the data controller may process personal data insofar as is necessary to achieve the purpose but may not process personal data he or she may do without. The application of the principle of proportionality is thus closely related to the principles of data protection from Article 5 GDPR.

B.5.1 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. As legal conditions they have to be complied with in order to make the data protection legitimate.[225] 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 informed about the processing of their data, that all the legal conditions for data processing are adhered to, and that the principle of proportionality is respected. Below, these conditions are elaborated in three subsections, focussed on the limited data processing by Nextcloud:

1. Lawfulness, Fairness and Transparency
2. Data minimisation and privacy by design
3. Storage limitation

B.5.1.1 Lawfulness, Fairness and Transparency

As described throughout part A of this DPIA, in boxes with mitigating measures taken by Nextcloud, Nextcloud has agreed to only process personal data when necessary and proportionate for the instructions given by the customer. This includes limited further processing for seven specific legitimate business purposes. As assessed in Section B.2.4 this further processing is compatible with the purpose for which the Dutch education organisations will instruct Nextcloud to process data as processor. This ensures that

[225] See for example CJEU, C-131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González, ECLI:EU:C:2014:317. Paragraph 71: *In this connection, it should be noted that, subject to the exceptions permitted under Article 13 of Directive 95/46, all processing of personal data must comply, first, with the principles relating to data quality set out in Article 6 of the directive and, secondly, with one of the criteria for making data processing legitimate listed in Article seven of the directive (see Österreichischer Rundfunk and Others EU:C:2003:294, paragraph 65; Joined Cases C-468/10 and C-469/10 ASNEF and FECEMD EU:C:2011:777, paragraph 26; and Case C-342/12 Worten EU:C:2013:355, paragraph 33).*

education organisations can comply with their obligation to ensure the lawfulness of the data processing by Nextcloud.[226]

As described in the part about compliance with legal obligations in Section A.7.3 Nextcloud has agreed to reject requests for disclosure from non-EU authorities, and take steps to prevent or minimise disclosure to EU authorities. Absent such an agreement, Nextcloud would have operated as a third party controller for such disclosures, and such disclosures would be unlawful under the GDPR (article 48) absent a mutual legal assistance treaty.

With regard to transparency, Nextcloud already provides reasonably adequate documentation about the contents of the audit and interaction logs that are (only) available for the customer.[227] Education organisations can use this umbrella DPIA to better understand and manage the data protection risks of unauthorised access to these logs. Additionally, Nextcloud has agreed to better support admins by providing a full list of available logs, and more detailed examples of the contents of the Talk interaction logs, as well as activities intentionally not registered by these logs in Q3 2026.

Nextcloud has made information available to SURF, as described in A.3.3.3 and A.3.5 about the (limited) logs it generates itself or through sub-processors like Postmark, Sendent, Zammad and DataCo. Nextcloud will make this documentation public in July 2026. SURF approves of the contents.

Additionally, Nextcloud used to include an invisible tracking pixel in its commercial and security mailings. The addition of an invisible tracking pixel to the newsletters was essentially unfair, as this constitutes obscurity by design. Nextcloud could have exported these observations about the individual reading behaviour of the recipients and potentially used these observations in a way that affects admins and procurement officers, but also other people that have registered for a Nextcloud event or have provided their contact data to download a whitepaper and are automatically subscribed to Nextcloud's commercial newsletter. Nextcloud did not inform potential or actual subscribers about this secretive tracking of reading behaviour. The lack of transparency and user choice made this data processing inherently unfair, and, without valid prior informed consent for the reading of this information from the recipient's devices, unlawful. In reply to questions from SURF Nextcloud has disabled the tracking pixel in the software with which it creates the newsletters.

Nextcloud does not publish a central source of information about retention periods of the different personal data, but it has agreed with SURF in the adapted DPA on the maximum retention periods for the processor data, as documented in Table 7 in Section A.11.2 and maximum retention periods of the authorised further processing purposes, as documented in Table 8.

Finally, as described in Section A.3.5 Nextcloud provides adequate documentation to admins about the first party cookies set by the self-hosted software, and will update the

[226] The lawfulness of the processing of Content Data on the tested services is out of scope of this umbrella DPIA: this is the responsibility of the Dutch government customers.
[227] Nextcloud, Logging, page undated, URL: https://docs.nextcloud.com/server/latest/admin_manual/configuration_server/logging_configuration.html (last visited 18 May 2026), in combination with more detailed information on the restricted access portal.nextcloud.com pages.

documentation of the functional cookies it sets on the restricted access websites. Nextcloud no longer sets analytical cookies without visitors' consent.

B.5.1.2 Data minimisation and privacy by design

The principles of data minimisation and privacy by default demand that the processing of personal data is limited to what is necessary: Data must be "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*" (article 5 (1) (c) GDPR).

This means that education organisations may not collect and store data (or allow Nextcloud to collect and store data) which are not directly related to a legitimate purpose. According to this principle, the default settings for the data collection should be set in such a way as to minimise data collection by using the most privacy friendly settings.

Nextcloud is commendable for having taken this principle to heart in 4 ways:

1. for the choice to have almost all data processing exclusively take place in the customer environment,
2. for (not collecting) Telemetry Data,
3. with regard to cookies its own website and on the main interface managed by the customer, and
4. for the scope of its audit and interaction logs.

As a result of the dialogue with SURF, Nextcloud has taken additional data minimisation measures, both relating to the data it collects itself, and with regard to the data the software collects.

Processing by Nextcloud GmbH

Nextcloud's core design principle for the Enterprise software, as often emphasised in the dialogue with SURF, is to know as little as possible from the customer, and to limit the data processing by the company Nextcloud to the absolute minimum. This philosophy has ensured that Nextcloud GmbH collects very limited pseudonymous personal data about the configuration of the software and about the number of active users.

In reply to observations about the Usage Survey, Nextcloud has changed its consent question and now offers admins an equal choice between Yes and No. Nextcloud has also changed the default setting and no longer asks admins every month to share the Usage Survey.

Both on the restricted access and publicly accessible relevant web pages, Nextcloud GmbH only sets functional cookies by default. As described in Section A.3.2 Nextcloud has committed to separate the admin account data from the Commercial Contact Data and offer a Do It Yourself subscribe and unsubscribe option for the different mailing lists via the restricted access portal page in Q3 2026.

If education organisations want to further minimise the (further) processing by Nextcloud of the admin Account Data in the Usage Survey and in the newsletter with security updates they can consider instructing admins to create pseudonymous accounts, like admin1[name organisation].nl.

Processing by the Nextcloud Enterprise software
Nextcloud's software does not collect Telemetry Data from users (admins and end users) accessing the software via their browser or installing it on their devices.

As quoted in Section A.3.3.1.1 about the audit logs and Section 0 about the interaction logs, Nextcloud logs events that are relevant for security purposes, and has intentionally refrained from logging excessive personal data, such as who voted what in a poll. Nonetheless some audit and talk interaction logs may contain some personal data, such as user names and file or room names. These personal data are necessary to strike the right balance between stability, security, privacy and maintainability. However, to help organisations limit access to these data internally, Nextcloud will create a second version of the audit logs for export to an internal SIEM, in which the personal data and sensitive data such as file and meeting names will be masked.

As described in the box with mitigating measures at the end of Section A.4.1 Nextcloud will enable admins to centrally enforce use of the lobby for all participants in a meeting. This helps the education organisations to only share personal data with authorised, preapproved, participants.

B.5.1.3 Storage limitation

The principle of storage limitation demands that personal data are only retained as long as necessary for the purpose in question. Data must be "*kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed*" (article 5 (1) (e), first sentence GDPR). This principle therefore demands that personal data are deleted as soon as they are no longer necessary to achieve the purpose pursued by the controller. The text of this provision goes on to clarify that "*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*" (article 5 (1) (e), second sentence, GDPR).

Like with data minimisation, storage limitation is relevant for the processing by Nextcloud GmbH, as well as for the education organisations, in the self-hosted Nextcloud Enterprise software.

Storage by Nextcloud GmbH
As quoted above in the analysis of the transparency of the data processing by Nextcloud GmbH, SURF and Nextcloud have agreed on maximum retention periods for the processor data, (Table 7 in Section A.11.2) and maximum retention periods for the authorised further processing purposes (Table 8). As a processor, Nextcloud retains the Account Data as long as the customer doesn't actively delete them. Nextcloud retains the identifiable Usage Survey data for one year and the data it collects via the support app for as long as the contract with the customer exists. Those retention periods seem long, but can be justified in view of the limited identifiable data. Nextcloud only collects a server IP address with the Support app, not an individual admin's IP address. And the Usage Survey contains an

Instance ID and a subscription ID which Nextcloud can link to an admin of an organisation, but the report does not include other (behavioural) details.

The retention periods for the System Information Report and the Website Data are very short: 14 days accessibility of the Report, seven days in the webserver access log, and the functional cookies have an expiry date of 30 days.

Nextcloud has also agreed to reduce the retention period of support tickets from 4 years after closure to 15 months for SURF-members. Generally, organisations need to motivate if they need to store solved tickets for longer than 13 months (sufficiently long to capture annually recurring incidents). Based on the amended DPA with SURF, customers can ask Nextcloud to delete single tickets and attachments or all tickets prior to the 15 months. Additionally, Nextcloud can use pseudonymised, aggregated support tickets as long as necessary to learn from past experiences and continue to improve the software and services.

The impact on data subjects becomes higher if the retention period is longer. In view of the temporary and agreed mitigating measures for the Support Data, and the specification and agreement in the amended DPA that Nextcloud only processes these personal data as a processor, these retention periods are proportionate.

Storage in the Nextcloud Enterprise software
To help education organisations comply with storage limitation requirements, Nextcloud has committed to offer customers an extra export option of the immutable audit and talk interaction logs by the end of 2026: export of the logs with personal data such as meeting and file names will be masked with ***REMOVED SENSITIVE VALUE*** for customers to import in their own log management tools.

In sum, Nextcloud is highly commendable for applying privacy by default both to its own data collection, and the processing in the Enterprise software, and for not collecting Telemetry Data. During the writing of this DPIA, Nextcloud has generously agreed to apply additional mitigating measures. Thanks to these measures, the data processing can be qualified as proportionate.

B.5.2 Assessment of the subsidiarity

The key question is whether the same goals can be reached with less intrusive means.

Nextcloud competes with two types of companies: (i) providers of cloud productivity software, and (ii) providers of alternative open source software.

SURF has previously assessed the compliance of the two main integrated productivity suites Google Workspace, and Microsoft 365 Office, and has negotiated GDPR-compliant contracts for the use of these services.

SURF has not yet performed a DPIA on other Office software, such as:

- Collabora Office (UK open source, based on LibreOffice),
- Euro-Office (spin off from OnlyOffice)[228]
- FreeOffice (German, not open source),
- LibreOffice (German, open source),
- OnlyOffice (Russian, open source), with
- Polaris Office (South Korean, not open source)
- Thinkfree[229] (South Korean, not open source, partner of Nextcloud)
- WPS Office (Chinese, not open source).[230]

There is no publicly available information that compares the compliance of all of these competing suppliers of Office software with privacy laws and regulations. However, Office software from Russia and China is unlikely to meet EU legal requirements or offer sufficient sovereignty controls.

As a German provider, Nextcloud has a unique advantage compared to its competitors from the USA (or the UK like Collabora). Nextcloud cannot be subjected to US American law (or UK law), including executive orders of the president. As described in Section A.8.1, SURF and the Dutch education sector have an essential interest in data sovereignty, to better prevent loss of confidentiality and sudden unavailability. The amended DPA with SURF includes limitative lists of purposes for all relevant personal data, excludes potential disclosure to government authorities outside of the EU and limits the engagement of sub-processors outside of the EU. Based on these terms and agreed processing limitations, Nextcloud realises the inherent benefits of being German and independently owned. Additionally, Nextcloud releases its software under the AGPL license. As described in the introduction of Section A.6 this license provides an important assurance for data sovereignty. Even if Nextcloud would be bought by a (non-EU based) competitor, nor Nextcloud nor the new owner can undo the open source nature of the software, and the copyleft assurance. In such circumstances, the open source development community is likely to create a 'fork', and start with the further open source development from that specific version onwards.

In sum, compared to the current use of competing cloud providers of Office productivity suites, with which SURF has already negotiated contracts, education organisations do not have experience with the use of Nextcloud as fully managed cloud service (by a partner of Nextcloud or by SURF as a central service), or experience with large scale *on-premises* deployment and management. However, based on the limited tests and the legal assurances in the amended DPA, Nextcloud can offer similar services with a higher level of data protection.

[228] GitHub, E-office, URL: https://github.com/Euro-Office. Since May 2026 Nextcloud includes Euro-Office as the default Nextcloud Office in the Enterprise All-In-One package, instead of Collabora Online.
[229] Thinkfree, How to set up Thinkfree Office for Nextcloud, last updated 16 March 2026, URL: https://cs.thinkfree.com/en/support/solutions/articles/158000282045-how-to-set-up-thinkfree-office-for-nextcloud .
[230] List based on current partners Nextcloud and Techradar, Best Microsoft Office alternative of 2026, 19 January 2026, URL: https://www.techradar.com/news/best-microsoft-office-alternative .

B.6 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 data processing agreement to include that the data processor will assist the data controller in complying with data subject rights requests.

As discussed in Section A.7.2 based on the amended DPA with SURF, Nextcloud qualifies as data processor for the processing of the limited Account, Diagnostic, Support and restricted access Website Data, with some exceptions when Nextcloud is authorised to process some personal data for agreed legitimate business purposes.

Both in a role as processor and as authorised controller Nextcloud commits to assist the controller with any data subject requests.

B.6.1 Right to information

Data subjects have a right to information. 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. As quoted above in Section B.4, the EDPB explains in its Guidelines on transparency that controllers should clearly explain the most important consequences of the processing.

"[n]atural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data."[231]

One of the purposes of this umbrella DPIA is to help education organisations that wish to use the tested Nextcloud services to better inform their employees about the agreed scope and purposes of the data processing.

As assessed in Section B.5.1.1, Nextcloud has provided important clarifications to SURF, and has improved its public cookie documentation. Nextcloud has agreed to publish extra information about the logs it collects itself (such as its webserver access logs and the logs collected by its sub-processors, including the retention periods, as well as about the functional cookies on the admin and support portals). Nextcloud will also help the admins understand that the audit and interaction logs can include personal data such as user names or room names.

As analysed in Section B.2.1 absent information about the use of tracking pixels in the newsletters, Nextcloud cannot obtain valid consent from its newsletter recipients. However, transparency is not sufficient to mitigate the risk of unlawful processing. As analysed in Section B.5.1.1 if Nextcloud switches to a different mail delivery provider in Q3 2026, it must prevent unlawful processing through the use of a tracking pixel or similar technology.

[231] The EDPB has adopted the Article 29 Working Party guidelines WP 260 rev 1, Guidelines on transparency under Regulation 2016/679, adopted on 29 November 2017, as last Revised and Adopted on 11 April 2018.

Based on this umbrella DPIA and the amended DPA education organisations that procure the tested services can inform their students and employees about the processing in the software, and the limited processing by Nextcloud. However, for prospective customers it is difficult to fully understand what personal data Nextcloud processes and for how long.

In sum, Dutch education organisations can comply with their obligations to provide their employees and students with adequate information about the scope and purposes of the data processing, if they use this umbrella DPIA and the amended DPA.

B.6.2 Right to access

Data subjects have a (fundamental) right to access personal data concerning them. 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.

Nextcloud undertakes as a data processor to assist its customers with such requests. As assessed in Section A.3.6 above SURF filed two Data Subject Access Requests (DSARs) per email.[232] Nextcloud replied within 8 days of submission, including several screenshots and a PDF explaining the data.

The response was detailed and easy to read. However, the reply was not always correct (any customer can always file a complaint with their national Data Protection Authority, customers are not required to contact an authority elsewhere in the EU), but more importantly, not complete.

The missing data were:

1. The Usage Survey Data - Nextcloud incorrectly claimed the report did not contain personal data, but was able to identify the admin via the IP address and the unique Enterprise license ID.
2. The activity logs about use of the Support Portal (Nextcloud must ask Zammad to provide access to the production log).
3. (Restricted access Websites) Webserver access logs – Nextcloud should have ‘frozen’ the data relating to the requesting data subject in reply to the DSAR (provided the data subject was able to provide relevant IDs for Nextcloud to reliably verify the identity of the data subject).
4. Logs kept by Sendent, Postmark and DataCo (about the new DSAR form opened after the tests by SURF were completed) and their retention periods.

Nextcloud did not explicitly refuse access to any personal data, and agreed to provide full access to all available personal data it processes as processor and as authorised

[232] Due to a misconfiguration of SURF’s test mail server, one of the mails didn’t reach Nextcloud.

controller, to the extent possible, if the data are still available and/or the data subject is able to provide the correct identifier for Nextcloud to retrieve the data.

In sum, Nextcloud commits to fully comply with its obligations to provide access. SURF has not filed a new DSAR to verify compliance, as this would have required retesting.

B.6.3 Right of rectification and erasure

Thirdly, data subjects have the right to have inaccurate or outdated information corrected, incomplete information completed and - under certain circumstances - personal information deleted or the processing of personal data restricted.

Education organisations can delete Content and Account Data, as well as the 1st and 2nd line support tickets in their own support ticketing systems. Customers can also limit the retention periods of logs in their own software (based on capacity). However, for security reasons it is recommended they export the available audit and interaction logs from the self-hosted software to their own log management systems. To help customers comply with data minimisation requirements and obligations to delete specific personal data if a user has filed a valid deletion request, or generally they no longer have a legal ground for the data processing, Nextcloud has committed to develop a second 'clean' version of the audit and interaction logs, by the end of 2026. In this second export version the personal data such as meeting and file names will be masked with ****REMOVED SENSITIVE VALUE****. Organisations can ensure access to the raw data in the original logs remain immutable (necessary for security purposes), but access is restricted to a root admin or another limited group of admins. Since the raw data in the original logs are not accessible via a GUI, the probability of unintentional access to personal data that should have been deleted is greatly reduced.

As assessed in Section B.5.1.3 above, Nextcloud's retention periods are generally proportionate and education organisations can ask for deletion of specific or all support tickets and attachments prior to expiry of the new (reduced) 15 months retention period. Additionally, Nextcloud (its sub-processor Zammad) will implement a banner in the support portal to warn admins not to upload personal data. These two measures ensure Nextcloud helps the education organisations to meet the requirements of Article 17(1)(a) and (d) of the GDPR. These provisions require a data controller to delete personal data without undue delay upon request of a data subject if they are no longer needed for the purposes for which they were collected or otherwise processed, or when the personal data have been unlawfully processed (in case an admin accidentally attaches confidential data to a support ticket).

In sum, based on the amended DPA Nextcloud allows education organisations to comply with their obligation to erase outdated or unlawfully processed data.

B.6.4 Right to object to profiling

Fourthly, data subjects have the right to object to an exclusively automated decision if it has legal effects. SURF has a specific contractual guarantee from Nextcloud that it does not use the personal data for profiling purposes. The only exception is that an admin can provide valid consent for tracking cookies on Nextcloud's publicly accessible website nextcloud.com.

B.6.5 Right to data portability

Employees have a right to data portability if the processing of their personal data is carried out by automated means and is based on their consent or on the necessity of a contract. As processor, some of the data processing by Nextcloud on behalf of education organisations could be based on the necessity of performing a (employment) contract with the admin and procurement officers. Nextcloud commits to comply with the right to data portability in the amended DPA with SURF.

However, the exercise of the right to data portability is not realistically possible for admins or procurement officers: as they would copy confidential data and personal data from the education organisation. Hence for data processed in their professional roles they cannot use this right to demand export of confidential data and personal data from the education organisation (Article 20(4) of the GDPR).

B.6.6 Right to file a complaint

Finally, education organisations as controllers must inform their employees and students about their right to complain, internally to their Data Protection Officer (DPO), and externally, to the Dutch Data Protection Authority (Autoriteit Persoonsgegevens). This is out of scope of this umbrella DPIA.

Part C Description and Assessment of Risks to Data Subjects

C.1 Risks to Data Subjects

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 as a result of the processing of the limited personal data by Nextcloud as processor, and as authorised controller. 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.

This part contains two different lists with risks and mitigating measures. The first list tentatively lists data protection and information security risks that can result from implementation and configuration choices made by the education organisation when deploying the Nextcloud Enterprise software.

The main analysis in Section C.2 analyses the probability and impact of the risks resulting from the data processing by Nextcloud, including default settings for the creation of logs with Diagnostic Data in the self-hosted environment and their retention periods, and takes all legal, technical and organisational measures into account that have been or will be applied by Nextcloud to mitigate identified risks.

C.1.1 Identification of risks

This DPIA identifies 15 specific data protection risks that result from the processing by Nextcloud, including software capabilities and configuration options for the education organisations.

The data protection risks can be grouped in the following categories:

- inability to exercise rights (including but not limited to privacy rights)
- inability to access services or opportunities
- loss of control over the use of personal data
- discrimination
- identity theft or fraud
- financial loss
- reputational damage
- physical harm
- loss of confidentiality
- re-identification of pseudonymised data or
- any other significant economic or social disadvantage[233]

These risks have to be assessed against the likelihood of the occurrence of these risks and the severity of the impact.

[233] List provided by the ICO, step 5, URL: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/

The UK data protection commission ICO provides the following guidance: *Harm does not have to be inevitable to qualify as a risk or a high risk. It must be more than remote, but any significant possibility of very serious harm may still be enough to qualify as a high risk. Equally, a high probability of widespread but more minor harm might still count as high risk.*[234]

In order to weigh the severity of the impact, and the likelihood of the harm for these generic risks, this report combines a list of specific risks with specific circumstances of the specific investigated data processing.

Table 10: Risk scoring matrix[235]

Severity of impact	**Serious harm**	**Low risk**	**High risk**	**High risk**
	Some impact	**Low risk**	**Medium risk**	**High risk**
	Minimal impact	**Low risk**	**Low risk**	**Low risk**
		Remote	Reasonable possibility	More likely than not
	Likelihood of harm (occurrence)			

C.1.1.1 Processing of personal data in the Nextcloud Enterprise software

As mentioned in the introduction of this section C, this section includes a tentative list of data protection and information security risks that can be mitigated by the education organisation themselves if they decide to self-host the Nextcloud Enterprise software.

This umbrella DPIA cannot provide an adequate overview of all potential internal data protection risks, related to the security configuration and the specific purposes for different categories of personal data that faculties/departments may want to use the software for, since these risks are highly dependent on the personal and confidential data that educations institutions will process in the Nextcloud software.

This umbrella DPIA can therefore only provide an overview of the general risks resulting from the use of Nextcloud. It is up to the privacy officers and DPOs to complement this umbrella DPIA with specific risks, and adapt adequate mitigating measures within each organisation. Therefore this section does not include an assessment of the probability and impact of the risks.

[234] Idem, step 5.
[235] As introduced by the ICO pre-Brexit, and copied by the Dutch government in its national DPIA template.

Table 11: potential risks for self-hosted software that can be mitigated by the organisations themselves

Potential internal data protection risks	Recommended mitigating measures
Loss of control / loss of confidentiality / loss of availability as a result of external data breaches (including phishing and ransomware)	Ask the CISO to create a risk assessment for the different categories of data based on the risk appetite of the organisation and implement all necessary measures (more than this tentative list)
	Ensure availability of capable system admins and 24/7 availability of a SOC.
	Study Section A.6.1 of this DPIA and implement available security measures.
	Regularly perform a penetration test on the self-hosted configuration.
	Export the Nextcloud logs to the organisation's own SIEM and other log management tools and perform systematic control on compliance.
	Ensure a back-up that cannot be compromised via the live system and ensure no personal data are processed in the Development and Test environment of the DTAP.
Loss of control as a result of internal data breaches	Consider use of the 13 privacy controls described in Section A.4.1
	Implement fine grained file access controls. Consider restrictions such as preventing access to XLSX files from the HR department by outside company IP ranges or blocking access to specific files from non-EU countries.
	Keep user registration in the AD/LDAP up-to-date, as access via groups depends on this registration.
	Inform end users about the 3 options they have to limit processing of their personal data (Section A.4.2).
Loss of control through lack of authorisation admins	Distinguish between root or top admins that can access the raw log data, and admins that can access masked logs in the organisation's SIEM and other log management tools.
	Update the internal IT policy to decide what data admins can share with Nextcloud (such as Usage Surveys and System Information reports).
Loss of control through lack of transparency	Use this umbrella DPIA and watch out for Nextcloud's agreed new public documentation to update the internal Register of Processing Activities, and update both the internal data processing policy/IT policy as well as the external privacy policy to inform all relevant data subjects about the data processing by the organisation itself and by Nextcloud.
Loss of control through excessive data retention	Clean up current data processing by deciding on a maximum age of files for import in the Nextcloud software. Update internal registration guidance and internal data

	processing manuals with maximum retention periods, and audit and enforce compliance.
Chilling effect employee monitoring system	- Discussed in the next section about risks caused and mitigated by Nextcloud.
Loss of control / loss of confidentiality unauthorised access to meetings	- Discussed in the next section: centrally enforce use of the lobby feature.
	Allow users to enable E2EE for meetings in Talk about confidential and sensitive topics.
Lack of assurance over software integrity, resulting in potential backdoors in software updates leading to unauthorised access or external data breaches.	Implement DTAP (Develop, Test, Acceptance, Production) segregation.
	Verify release integrity using signatures and cryptographic hashes before deployment.
	Enable centralised logging and SIEM monitoring for detection of anomalous activity or data exfiltration.

C.1.1.2 Processing of personal data by Nextcloud (including design decisions)

As a result of the negotiations with SURF, Nextcloud has factually and formally become a data processor for the (limited) personal data in the Admin Account Data, Diagnostic Data, Support Data and restricted access Website Data. Nextcloud is also authorised in the amended DPA to further process specific personal data for seven legitimate business purposes, when strictly necessary and proportionate. These contractual improvements have mitigated many high data protection risks related to a loss of control and lack of purpose limitation.

Nextcloud prides itself on its open source data processing, enabling EU customers to fully control the data processing within the EU. However, it follows from this DPIA that in the set-up tested by SURF, Nextcloud currently uses one US American sub-processor (ActiveCampaign), and customers can choose partners outside of the EU, such as Collabora in the UK. Nextcloud also makes customers visit the websites of two US American third parties (GitHub and Hugging Face) to download software and necessary security updates. Nextcloud has committed to switch to an EU-based mail delivery provider in Q3 2026 and has agreed to other mitigating measures.

Nextcloud has ensured the software generates sufficient logs for customers to comply with their security obligations. These logs can include sensitive data, what student or employee signed in when, and what files they worked on. To help education organisations prevent unnecessary access to these logs, Nextcloud has committed to create a masked version of the audit and interaction logs for export in the more generally accessible log management systems in an organisation. This measures protects against the chilling effect on users and admins that they fear that their behavioural data are monitored.

Finally, Nextcloud has committed to distinguish between admin Account Data and Commercial Contact Data, and will only send newsletters with the specific consent from admins and commercial contacts, thus preventing the risk of loss of time and annoyance

because of unsolicited mail. Nextcloud has also stopped using a tracking pixel in its newsletters.

In all, the observed processing of the Account, Diagnostic, Support and Website Data by Nextcloud, as well as Nextcloud's decisions in the software for the processing of Diagnostic and Website Data results in **15 low or mitigated data protection risks.** Based on the adapted new DPA with SURF and other measures Nextcloud has taken or will take, all of these risks have been mitigated, can be mitigated by the education organisations, or will soon be mitigated by Nextcloud (by the end of 2026 the latest).

C.2 Assessment of risks

C.2.1 Loss of control purposes processing of admin Account Data in Account, Diagnostic, Support metadata and Website Data

As described in Section A.3.2 Nextcloud did not distinguish between admin Account Data and Commercial Contact Data. Nextcloud qualified itself as data controller for both types of contact data and credentials. As controller Nextcloud permitted itself to process these combined data for its own purposes.

Since the education organisations factually enable Nextcloud to process the admin account data, and the admins do not have a choice but to log-in to the admin and to the support portal to perform their work duties, the data processing by Nextcloud is inextricably linked to the processing for which the education organisations want to use the Nextcloud Enterprise software. Therefore, as argued in Section A.7.4 Nextcloud was not an independent data controller for this data processing, but a joint controller (or at the very least, a third party from the perspective of the education organisation). Education organisations do not have a legal ground to disclose admin Account Data to a third party. Without an explicit authorisation from the education organisations the further processing by Nextcloud as controller would not be compatible with the processor purposes.

SURF and Nextcloud have agreed on a limitative list of processor purposes, and a limitative list of authorised further processing purposes. Nextcloud is a processor for admin Account Data (also when included in the Diagnostic, Support and restricted access Website Data). Section B.2.4 assesses that the authorised further processing of the aggregated admin Account Data for compliance with legal obligations, and in statistical form for internal reporting, financial reporting and product strategy and to technically improve and optimise the performance and efficiency of the software is compatible with the agreed processor purposes.

As admin Account Data are sensitive from the perspective of their access to multiple personal data from end users, as described in Section A.2.2.2, the impact of incompatible further processing would be high. However, based on the amended DPA, Nextcloud has reduced the probability of occurrence to near-zero. Therefore this risk can be qualified as solved.

C.2.2 Loss of control transfer of email addresses to the USA

As described in Section A.7.2.2 as controller Nextcloud has decided to engage a mail delivery provider from the USA (ActiveCampaign, brand name Postmark) as processor for all of its outbound mail. As analysed in Section A.9.1 this leads to a data transfer of the admin Account Data and Commercial Contact Data that are automatically subscribed to newsletters, as well as the contents of the outbound mail to the USA (stored in a log file for 45 days). Even though the EC decision is formally still valid that the USA have an adequate level of data protection, SURF considers digital sovereignty to be necessary to uphold and protect values such as privacy, autonomy and inclusion, as described in Section A.8.1.[236] Nextcloud also positions itself as the best partner for EU data sovereignty, as described in Section A.8.2.

Potential disclosure by ActiveCampaign/Postmark of the two types of contact data from Dutch education organisations to government authorities in the USA could have a high impact, in particular if admin Account Data are subsequently used for spear phishing, to gain access to more data stored in the Nextcloud Enterprise software. However, in reply to SURF's concern about this data transfer, Nextcloud committed to switch to an EU native mail delivery provider in Q3 2026. Once this switch has been completed, the probability of unauthorised access by government authorities in the USA is zero, since Nextcloud has also contractually agreed with SURF to always reject requests from non-EU authorities. Therefore, by Q3 2026 this risk can be qualified as low.

Additionally, admins of education organisations will frequently have to visit the US American owned and hosted repository GitHub for Nextcloud security advisories and to download updates, and maybe Hugging Face to download the Whisper LLM as part of the tested Talk generative AI transcription solution. To mitigate the risk of compelled disclosure to US government authorities by these two third parties, admins should prevent sharing their private IP addresses and personal device details when accessing these sources, for example by using a VPN and/or erasing cookies and local storage and prevent leakage of a device fingerprint. Foremost, admins should not remain permanently logged-in to GitHub and Hugging Face.

C.2.3 Loss of control transfer Support Data Collabora outside of the EU

In the test set-up for this DPIA, SURF used Nextcloud Office as office suite. Nextcloud also offers supported access to other office document editing suites, from ONLYOFFICE, ThinkFree Office and the on-premises Microsoft Office.[237]

As described in Section A.1.2.1 Nextcloud Office is a frontend for the Collabora Online software from the UK company Collabora. If an education organisation asks Nextcloud for support relating to Nextcloud Office, the ticket is accessible for employees from the Collabora company. As described in Section A.9.1 per request of SURF Nextcloud has ensured that access for employees of Collabora to the relevant support tickets in Zammad is limited to employees physically located in the EU and the UK. Nextcloud has committed to limit the access to EU based employees if the adequacy decision for the UK becomes

[236] Idem.
[237] Nextcloud reply to part A of this DPIA, 2 April 2026.

invalid. Nextcloud itself also has collaborators based outside of the EU, but had already technically restricted access to employees physically located in the EU (see Figure 35).

Potential unauthorised disclosure of support conversations and metadata to government authorities outside of the EU, where Collabora employees are located, could have a high impact, if that information can be used to subsequently (spear-)phish an admin or otherwise corrupt the integrity of the software. However, thanks to these two mitigating measures, Nextcloud has reduced the probability of occurrence to near-zero. Therefore this risk can be qualified as solved.

C.2.4 Loss of confidentiality through lack of 2FA on support portal

As described in the security assessment in Section A.6.1 Nextcloud offers an admin and a support portal via a website maintained by its (German) subprocessor Zammad. Nextcloud does not yet require two factor authentication to sign on. Absent this measure, it is easier for malicious actors to access these restricted access pages and compromise admin accounts.

Nextcloud has worked with Zammad to solve this issue, and has committed to enforce 2FA on the admin and support portal in the new version v7.1 of Zammad's support portal that has been released on 1 July 2026. Even though the impact of admin account breaches can be high, Nextcloud has effectively reduced the probability of occurrence to low. Once Nextcloud has completed testing and releases the new portal version, the risk is solved.

Note: to help organisations that decide to self-host the Nextcloud Enterprise software, SURF has created a provisional table with necessary security measures in Section C.1.1.1.

C.2.5 Loss of control through lack of transparency Diagnostic Data

Even though the Nextcloud Enterprise software is designed to enable customers to manage and control the data processing themselves, it follows from the technical network traffic data analysis described in Section A.3.3 that the company Nextcloud GmbH can optionally collect and processes 3 types of Diagnostic Data from admins, via the Usage Survey, the System Information Report and data that are automatically shared via the support app.

The logs contain pseudonymous data like unique customer (organisation) or device IDs, and/or IP addresses relating to a specific organisation, plus configuration details or statistics about the number of users (identifiable for the education organisations). Since Nextcloud also has admin Account Data and Commercial Contact Data, Nextcloud is technically capable of relating these data to identifiable individuals within the customer organisations. Nextcloud does not provide public documentation about the contents of these logs.

Based on the amended DPA with SURF, Nextcloud has become a processor for these Diagnostic Data, and will only process these data in identifiable form for the four agreed purposes. Nextcloud has also improved the choice for admins whether to share the Usage Survey data or not. To further minimise the data flow to Nextcloud, education organisations can consider use of pseudonymised admin employee accounts, for example using identity federation, when they decide they want to share Usage Survey Data with Nextcloud.

As described in Section A.11.2, Nextcloud has committed to document the processing of Diagnostic Data (Usage Survey, System Information Report and support app data) and publish defined retention periods for these data. The amended DPA also includes the retention periods of these 3 reports with identifiable data.

Prior to the negotiated DPA, the retention periods of these logs were unknown. The longer data are retained, the higher the potential impact in case of unauthorised access. However, based on the amended DPA and Nextcloud's commitment to publicly document these retention periods, the probability of a loss of control is remote. Therefore this risk can be qualified as low.

C.2.6 Loss of control through lack of transparency and risk of reidentification other Diagnostic Data, support system activity log, and Website Data

Besides the three types of Diagnostic Data Nextcloud collects via admins (see Section C.2.5 above), Nextcloud can remotely create seven types of logs with personal data that are not accessible for admins (see Section A.3.3.3):

1. Software download and update log
2. Push notification proxy log
3. Activity log in Zammad's support ticketing system
4. Webserver access log (visits to the restricted access Support Hub website, to portal.nextcloud.com, and Nextcloud's publicly accessible nextcloud.com website)
5. Log of outbound email to customers including newsletters (via ActiveCampaign / Postmark)
6. License distribution log (via Sendent, only in this specific test scenario[238])
7. Log of privacy / access requests (via DataCo)

Nextcloud does not provide public documentation about the contents of these logs. Nextcloud has provided SURF with additional information and has committed to publish information about the processing of these seven logs with the retention periods. SURF has reviewed this documentation, and assesses this to adequately remedy the lack of transparency.

On the restricted access portal and support pages, Nextcloud by default only sets functional cookies (no analytical cookies), but fails to document these cookies. As shown in Table 7, Nextcloud only retains the webserver access log for seven days, and does not store the cookie data beyond the end user browser.

To further lower the probability of a loss of control, SURF and Nextcloud agreed that Nextcloud generally acts as processor for these seven logs, except for the log of outbound email to commercial contact data (when Nextcloud acts as authorised data controller). On behalf of the education organisations, SURF can exercise the right to audit Nextcloud's compliance with the provisions in the amended DPA. This right to audit includes both the

[238] In reply to questions from SURF about the data processing by Sendent, Nextcloud explained: "*This is not a default. Sendent develops optional components that can be bought on request. If you purchase Nextcloud Enterprise in the Ultimate plan, their products are included and therefore will be provided in addition to our license*." Reply Nextcloud 6 May 2026. To provide SURF with a single Enterprise test license, Nextcloud also used Sendent.

processing by Nextcloud as processor, and the processing by Nextcloud as authorised controller.

In reply to the technical cookie findings, Nextcloud updated the cookie information about its public website and corrected an error. Education organisations should instruct admins not to change the default privacy friendly cookie settings on the public nextcloud.com website.

An absence of transparency negatively impacts the ability of admins to exercise their right to data subject access. However, based Nextcloud's new documentation (as approved by SURF) the probability of loss of control is remote. Therefore this risk can be qualified as low.

C.2.7 Loss of control and lack of transparency sub-processors

As described in the factual analysis of Nextcloud's GDPR role based on its public contract documentation (Section A.7.2.2) Nextcloud does not give its customers control over the (sub-) processors it engages. However, based on the amended DPA with SURF, Dutch education organisations can exercise this control through a number of contractual measures. Nextcloud commits to only engage subprocessors that process personal data in the EU, with two temporary exceptions (the US American mail delivery provider and employees of Collabora in the UK). The amended DPA with SURF also ensures Nextcloud gives the education organisations 60 business days advance notice (except in emergency situations) before the engagement of new sub-processors.[239]

Even though the impact of the engagement of unauthorised (sub) processors could be high, Nextcloud has effectively reduced the probability to near-zero. Therefore this risk is solved.

C.2.8 Inability to exercise data subject access rights

As described in Section A.3.6 and assessed in Section B.6.2, Nextcloud provided a swift and detailed response to the DSARs filed by SURF. However, the reply was not always correct (omitted to mention the national Dutch DPA), but more importantly, not complete. Nextcloud did not explicitly refuse access to any personal data, and agreed to provide full access to all available personal data it processes as processor and as authorised controller, to the extent possible, if the data are still available and/or the data subject is able to provide the correct identifier for Nextcloud to retrieve the data.

The impact of an unjustified refusal to provide access would have a very high impact, as the right to data subject access enables data subjects to understand the legitimacy of the data processing, and based on the reply, exercise other rights, such as the right to ask for deletion of personal data. However, based on Nextcloud's commitment to provide full access to all available personal data, the probability of occurrence is near-zero. Therefore, the risk can be qualified as low.

C.2.9 Inability to exercise data subject rights to delete Support Data

Nextcloud's user interface of the Support Portal does not offer options to admins to delete individual or multiple support tickets or attachments. As described in Section A.3.4 and assessed in Section B.5.1.3, Nextcloud initially retained closed support tickets for 4 years.

[239] Nextcloud DPA template, Section 7.7, Use of Sub-processors.

As a processor, it is not up to Nextcloud to determine this retention period, but to the data controller, the education organisation. Generally, organisations need to motivate if they need to store tickets with identifiable data for longer than 13 months (enough to capture annually recurring incidents). Based on the amended DPA with SURF, Nextcloud can use pseudonymised, aggregated support tickets as long as necessary to learn from past experiences and continue to improve the software and services, but this instruction does not apply to the directly identifiable data.

Nextcloud has agreed to reduce the retention period to 15 months for SURF-members, and customers can ask Nextcloud to delete single tickets and attachments or all tickets prior to the expiry of this reduced retention period. Nextcloud has already added a warning for admins on portal.nextcloud.com not to upload any personal data in attachments and Nextcloud has agreed with Zammad to implement the same warning on support.nextcloud.com in Q3 2026.

Even though the impact of an inability to exercise the right to deletion formally qualifies as a very high risk, given the importance the GDPR attaches to the exercise of fundamental rights, the reduced retention period, the warnings and the option to ask Nextcloud to delete tickets together lower the probability of occurrence of the risk of the inability to delete personal data to remote. Therefore this risk can be qualified as low.

C.2.10 Loss of control disclosure (limited) personal data to public bodies in and outside of the EU

Nextcloud GmbH collects limited personal data. And as a German company under exclusive German ownership, Nextcloud GmbH is not directly subjected to US American or other non-EU law. These circumstances already make it improbable that Nextcloud GmbH could be compelled by non-EU government authorities to disclose personal data relating to Dutch education customers. Nextcloud has confirmed it has never received a request for disclosure.

However, the company does sell its software to customers outside of the EU. As described in Section A.5.2.2 (purpose of compliance with legal obligations) there is a (theoretical) risk that Nextcloud GmbH could be forced (blackmailed) to stop providing the software to one or all EU customers. The US government could put the entire company Nextcloud GmbH on one of its sanction lists if it continued to provide services to a sanctioned person or organisation in the USA or elsewhere. Such a sanction would ban US customers from purchasing Nextcloud Enterprise services, and thus economically blackmail Nextcloud in compliance with extraterritorial law. Nextcloud answered that this type of blackmail would not work, since US customers only account for a small portion of revenue, and the sane business decision would be to cease the US operations.

To further cement the low probability of occurrence of this risk, Nextcloud has agreed to four contractual measures/commitments in de amended DPA with SURF:

1. Nextcloud will unconditionally reject requests from non-EU authorities.
2. Nextcloud will minimise the data it can be compelled to disclose to EU authorities. Nextcloud will conduct a thorough legal review of any request if it is prohibited from

forwarding the request to the customer, and object to the request as a matter of principle.
3. Nextcloud will publish annual transparency statistics, about the number of requests and the number of times it has disclosed any data.
4. Nextcloud has not purposefully created any “backdoors” or similar programming in the Software that could be used by third parties to access the system and/or personal data, or changed its business processes, or is subjected to any law that would require it from introducing backdoors.

These commitments further reduce the probability of occurrence to near-zero. Even though the impact of potential disclosure to non-EU authorities can be high, the risk can be qualified as low.

C.2.11 Loss of control processing Nextcloud independent controller

Prior to the amended DPA with SURF, Nextcloud qualified itself as an independent data controller for all data processing except for the contents of support tickets. As analysed in Section A.7.4 the data processing was governed by Nextcloud’s Privacy and Legal Policy.

Based on article 28(10) of the GDPR processors that take decisions themselves about the purposes of the processing illegitimately become controllers. However, Nextcloud could not be qualified as an independent data controller, but had to be qualified as a de facto joint controller with the customer that enables the processing by using the Nextcloud Enterprise software.

Nor SURF nor Nextcloud wanted to enter into a joint controller agreement to specify the purposes of the processing and the exercise of data subjects rights. Instead, Nextcloud agreed to include a limitative list of seven authorised further processing purposes in the DPA. As shown in Section B.2.4 SURF has assessed that further processing for these purposes is compatible with the original data collection purposes. Additionally, Nextcloud has agreed to separate the admin Account Data from the Commercial Contact Data, to prevent confusion about Nextcloud’s role as processor for the admin contact data, and Nextcloud’s role as authorised controller for the Commercial Contact Data.

Even though Nextcloud in its role as controller does not mention any high risk purposes of the data processing in its Privacy and Legal Policy, the impact of unauthorised further processing of the admin Account, Support and Diagnostic Data for Nextcloud’s own purposes still had to be assessed as medium. However, based on the amended DPA with SURF, including the agreement on the privacy by default settings of the public website, the occurrence of the risk of a loss of control over the controller purposes is near-zero. Therefore this risk can be qualified as solved.

C.2.12 Loss of control: use of tracking pixel in Nextcloud outbound mail

As described in Section A.10, Nextcloud added a tracking pixel to all outbound email. With the help of these invisible 1x1 pixels Nextcloud collected interaction data, such as reading, opening or clicking on its newsletters.

Nextcloud did not document this data processing, nor asked users to consent. Following earlier advice from the data protection authorities in the EU united in the Article 29 Working

Party, the EDPB has also explained the use of tracking pixels falls in the scope of Article 5(3) of the ePrivacy Directive. Hence, prior informed consent is required, as well as an option to reject the data processing.

The lack of transparency made this processing inherently unfair, as assessed in Section B.5.1.1. This intransparent processing had limited impact as the surveillance only involved business communication, but the impact of secret surveillance cannot be assessed as negligible. To mitigate this risk education organisations could only recommend admins to disable downloading pictures in their webmail, but such an organisational measure is far less effective than a technical measure.

However, in reply to this analysis Nextcloud has disabled the tracking pixel. This reduces the probability that admins reveal their reading behaviour to zero. The impact is similarly reduced to zero. Therefore, this risk has been solved.

C.2.13 Loss of control Admin account data in newsletters

Prior to the negotiation of a amended DPA with SURF, Nextcloud considered itself to be an independent controller for the admin Account Data it collects together with the commercial contact data, or when they subscribe to one or more newsletters. As assessed in Section C.2.1 admin Account Data are sensitive from the perspective of their access to multiple personal data from end users. As described in Section A.2.2.2 the impact of incompatible further processing would be high.

To prevent occurrence of the risk of a loss of control over these admin Account Data, Nextcloud has agreed to two technical measures: to clearly distinguish between the admin Account Data and the Commercial Contact Data and to build a Do It Yourself portal to subscribe and unsubscribe to newsletters, both in Q3 2026.

In view of these measures, the probability can be lowered to remote and the risk can be classified as low.

C.2.14 Loss of control through lack of transparency existence of multiple logs in the software

Nextcloud generated many different logs in the self-hosted software. Access to these logs is essential for organisations to comply with security obligations, and to monitor for data exfiltration or detection of anomalous activity. Additionally, organisations need to prevent excessive data retention periods. The contents of the audit and interaction logs with personal data as analysed by SURF are adequate (see Sections A.3.3.1.1 and 0), but SURF noticed the availability of at least 14 other logs (see the list at the end of Section A.3.3). The availability, contents and default retention periods of these logs are not sufficiently well-documented.

Nextcloud has yet committed to publish central information about the existence of the different logs for admins, and to better explain when Nextcloud logs can record sensitive and identifying information in the audit and talk interaction logs, in Q3 2026.

Education organisations can already use this DPIA to inform admins and update their Register of Processing Activities (ROPA), and will soon be able to also use new central

documentation from Nextcloud. The impact of a lack of transparency could be non-negligible, as some logs may be retained too short to detect anomalies, especially if a data breach remained undetected, other logs retained too long. Nextcloud's commitment lowers the probability that future customers are unaware of the existence and retention period of logs to remote. Therefore this risk can be qualified as low.

C.2.15 Chilling effect: employee and student monitoring system

Education organisations have access in their self-hosted software to audit and interaction logs with information on the specific actions and documents accessed by end users, and login patterns, as described in Section A.3.3.1.1 and 0. The logs contain directly and indirectly identifying data. Some of these logs contain Content Data, such as names of files, or names of (removed) meeting rooms.

Based on these logs admins can monitor individual working and study behaviour. If education organisations were to use these Diagnostic Data as employee and/or student monitoring system, the impact could be very high. The knowledge that an employer can process detailed usage data for evaluation purposes can have a *chilling effect* on teachers and students using the Nextcloud Enterprise software. They may fear that the monitoring could be used for a negative performance assessment, if not specifically excluded in an (internal) privacy policy for the processing of employee and student personal data. Such monitoring can prevent them from a legitimate exercise of related fundamental rights such as the freedom to send and receive information.

To help organisations prevent this risk, Nextcloud has agreed to create a second export of the audit and interaction logs by the end of 2026, in which the user names and content data are masked with ***. Organisations can import these redacted logs in their own log management system. This solution strikes a balance between the necessity of immutable audit logs to record all activities, including malicious activity erasure activities, and the obligation under the GDPR to minimise the risks for data subjects of excessive, unnecessary data processing.

In the context of the Dutch education sector, the probability that that this data processing leads to chilling effects is remote. This DPIA assumes education organisations follow the recommendation to limit access to the raw audit and interaction logs to the absolute minimum, and only use the redacted logs for day-to-day software management and security monitoring.

Furthermore, this DPIA assumes that education organisations will implement an internal privacy policy with rules and legitimate, specific purposes for the (further) processing of the logs with the raw data, including monitoring of the access by (global/root) admins to these raw data.

Assuming education organisations implement and verify compliance with an adequate internal privacy policy, the risks for data subjects can be qualified as low.

Table 12: Assessment of the 15 identified risks

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

Part D Description of Proposed Mitigation Measures

D.1 Mitigation Measures

The following section contains a table of the technical, organisational and legal measures that need to be, or have already been taken by Nextcloud and by the education organisations (including the provider of their fully managed solution) to mitigate the 15 identified data protection risks.

D.1.1 Suggested and taken measures to mitigate risks

This table shows the recommended measures for education organisations, the recommended measures for Nextcloud and the measures taken or committed by Nextcloud as a result of the new contract with SURF.

Provided the education organisations implement the recommended measures, all 15 identified risks are mitigated (solved in the table) or can be reduced to a low risk.

Table 13: Overview of data protection risks, mitigating measures and residual risks

No.	Risks	Recommended measures education organisations	Measures taken or committed by NEXTCLOUD	Residual risks
1.	Loss of control purposes processing of admin Account Data in Account, Diagnostic, Support metadata and Website Data	Sign up for Nextcloud Enterprise via SURF, and when signing up via a reseller or provider of a fully managed solution, ensure applicability of the SURF DPA.	Agreed to limitative list of 4 processor purposes in amended DPA.	solved
			Agreed to limitative list of seven authorised further processing purposes (legitimate business operations) in amended DPA.	
			Agreed to 3 explicit processing prohibitions: no further processing for other purposes, no processing for advertising purposes or serve advertising, not for direct marketing, profiling, research or analytics purposes unless the customer instructs Nextcloud to do so, no CSAM scanning.	
		(SURF): use the audit right to verify compliance with purpose limitation, data minimisation and retention periods.	Agreed to extensive audit right for SURF on behalf of the education organisations in amended DPA.	
			Committed to renew the security code audit for CSPN every 3 years and share the full findings with SURF.	

2.	Loss of control transfer of email addresses to the USA	-	Committed to switch to an EU-based mail delivery provider in Q3 2026.	low
		Instruct admins to prevent sharing their private IP addresses and personal device details when accessing GitHub and Hugging Face.	Nextcloud as a processor only processes data in the EU as agreed in amended DPA, with the exception of subprocessors outside of the EU chosen by customers such as Collabora.	
		Instruct admins to not remain permanently logged-in to GitHub and Hugging Face.	Nextcloud will offer two types of subscription to Enterprise customers in Q3 2026: as commercial contact for a customer or as admin.	
3.	Loss of control transfer Support Data Collabora outside of the EU	-	Limited the access to the relevant Collabora tickets in Zammad to employees physically located in the UK and in the EU.	solved
			Committed to prevent access from employees located in the UK if the adequacy status becomes invalid.	
4.	Loss of confidentiality through security breach	-	Nextcloud will enforce 2FA on the admin and support portal in the new version v7.1 of Zammad's support portal which has been released 1 July 2026.	solved
5.	Loss of control through lack of transparency Diagnostic Data optionally shared by admins	Optional: consider use of pseudonymised admin employee accounts, for example using identity federation to share Usage Survey Data with Nextcloud	Agreed to include Diagnostic Data in expanded scope of the amended DPA.	low
			Retention periods of 3 types of logs optionally shared by admins agreed in amended DPA,	
			Will publicly document these retention periods in July 2026.	
		(SURF): conduct audits on compliance with purpose limitation, data minimisation and retention periods both as processor and as authorised controller.	Agreed to extensive audit possibilities for SURF in amended DPA.	

6.	Loss of control through lack of transparency and risk of reidentification other Diagnostic Data, support metadata, and Website Data	Inform admins about the functional cookies with this umbrella DPIA and instruct them not to change the default settings on the public nextcloud.com website.	Will update information about functional cookies on admin and support portal in July 2026	low
		Inform admins about the existence of the seven identified relevant logs generated by Nextcloud GmbH and its sub-processors and the retention periods.	Nextcloud has provided SURF with additional information about the seven logs. Nextcloud will publish this information on its public website in July 2026 (as approved by SURF).	
		Inform admins about the contents of the Zammad support ticketing system's activity log and retention period of 42 days.	Nextcloud will publish this information on its public website in July 2026 (as reviewed by SURF).	
7.	Loss of control and lack of transparency sub-processors	-	Agreed to procedure to deal with changes in amended DPA, both with regard to new subprocessors and to other changes.	solved
8.	Inability to exercise data subject access rights	-	Committed to provide full access to a DSAR. This includes access to any collected Usage Survey Data, activity logs from the support ticketing system, frozen webserver access logs (provided Nextcloud can reliably verify the identity of the data subject) and logs kept by Postmark (or future EU based mail service provider). *NOTE: SURF has not retested this with a new DSAR.*	low
9.	Inability to exercise data subject rights to delete	Instruct admins to only share strictly necessary personal data in support tickets. Do not use support tickets to	Nextcloud will generally honour requests to delete one or more support tickets and/or attachments, unless there is a legal reason to retain a specific ticket.	low

	Support Data	file legal or financial claims.	Nextcloud has agreed on a maximum retention period of 15 months for closed support tickets for SURF members.	
			In the agreed new public documentation about the logs Nextcloud GmbH collects and retention periods Nextcloud includes it can exceptionally retain the support tickets about a specific topic longer, for a specific legal reason.	
			Nextcloud has already implemented a warning against sharing of personal data in attachments on the admin portal, and will show the warning in the support portal by Q3 2026.	
		Instruct admins to annually ask Nextcloud for deletion of all support tickets after the self determined retention period of for example 13 or 15 months.	Agreed in amended DPA to only process aggregated and pseudonymous data higher than tenant level from support tickets as authorised controller.	
10.	Loss of control disclosure (limited) personal data to public bodies in and outside of the EU		Agreed in amended DPA to proposed risk minimisation steps. Nextcloud will reject requests from non-EU authorities. Nextcloud will try to redirect requests from EU authorities to its customer, legally contest where possible and viable, but if necessary, only disclose the minimum necessary data.	low
			Committed in amended DPA to publish transparency statistics at least once a year, including numbers about received and answered requests.	
11.	Loss of control	Warn admins not to use their Admin	Agreed to two lists of purposes in amended DPA.	solved

	processing Nextcloud independent controller	Account Data to enable processing by Nextcloud or third parties as independent controller, for example by consenting to analytic and tracking cookies. Tell admins to use a pseudonymous account when registering for an event or when registering to download a whitepaper.	Agreed in amended DPA to maintain current privacy by default settings. Analytics and marketing cookies are only placed on the public website after voluntary consent of the user.	
12.	Loss of control: use of tracking pixel in Nextcloud outbound mail	.	Nextcloud has disabled the tracking pixel in its mailings.	solved
13.	Loss of control Admin account data in newsletters	Instruct admins to unsubscribe from commercial newsletters	In the self-service Nextcloud portal (portal.nextcloud.com) customers will be able to register as admin or commercial contact and decide themselves to subscribe and unsubscribe to commercial and technical newsletters in Q3 2026.	low
14.	Loss of control through lack of transparency existence of multiple logs in the software	Use the list in this umbrella DPIA to make admins aware of all available logs.	Nextcloud will provide a better overview of available logs for admins in the existing log documentation in Q3 2026.	low
15.	Chilling effect: employee and student	Make admins aware of the potentially sensitive contents of the (original) audit and Talk interaction logs.	Nextcloud has committed to develop a second export version of the audit and interaction logs, by the end of 2026. Personal data such as meeting and	low

	monitoring system	Update the internal IT policy when these logs can be legitimately used for what purposes.	file names will be masked with ***REMOVED SENSITIVE VALUE***.	
		To prevent use of the audit and interaction logs as employee monitoring system, import the masked version of the Audit and Talk interaction logs in the SIEM and log management tools once available and determine an adequate retention period for the raw data.	Nextcloud will update the available information about the sensitive contents in Q3 2026.	