Driving innovation together

DPIA TOPdesk

SURF Vendor Compliance

Author(s)): Arnold Roosendaal, Winfried Tilanus, Evan Blommaert

Version: 1.0
Date: 15 januari 2026

Version management

Version	Date	Comments
0.1	13/08/2025	First draft part A by Privacy Company
0.2	26/09/2025	Second draft part A by Privacy Company
		First draft parts A – D by Privacy Company
0.3	12/11/2025	Second draft parts A – D by Privacy Company
0.9	27/11/2025	Final draft parts A – D by Privacy Company
0.95	02/12/2025	Minor changes to Final Draft, Included TOPdesk response
0.96	12/12/2025	Removal of a medium risk on data subject requests, as it was based on incomplete information.
1.0	15/01/2026	NDA-check and publishing

TOPdesk’s response to this DPIA

We sincerely thank SURF and Privacy Company for thoroughly reviewing our product and services and for bringing these issues to our attention. Their detailed analysis helps us further strengthen our privacy and security measures.

We are pleased to report that many identified risks have already been mitigated. We have improved our notification procedures for Sub-Processors changes, created a more detailed policy regarding personal data in log files, and improved the procedures for handling Data Subject requests. These measures have already reduced several risks from high or medium to low, and we are actively working to resolve the remaining items. Our commitment is to ensure all outstanding risks are mitigated by the end of 2026.

Customers using TOPdesk can rest assured that, while some high risks are currently open, they are unlikely to result in any noticeable impact to individuals. The currently unmitigated risks primarily relate to technical or procedural aspects that are very unlikely to directly affect the rights and freedoms of end users. We urge all customers to check if their TOPdesk environment is implemented in line with the privacy (KI 9624) and security (KI 16810) best practices mentioned in our knowledge base to further reduce the risk.

We’d like to highlight several positive findings from the report:

- TOPdesk has shown transparency and proactive engagement throughout the audit process, quickly addressing issues as they arose.
- TOPdesk offers robust privacy features, including anonymisation, granular authorisation management (both for end users and our colleagues), and strong data separation between customers.
- Our security measures provide a high level of assurance for data protection, such as encryption at rest and in transit, regular vulnerability scans, and regular SOC2 audits.
- Our suppliers (Microsoft and Cloudflare) fully supported our GDPR compliance efforts and helped us improve response times for future data subject access requests.

We thank our suppliers for their cooperation and ongoing support. Their partnership has been crucial in ensuring we meet the highest privacy and security standards for our customers.

While responding to the auditors’ initial findings, we found the help of our colleagues at Support, Development, and the SaaS hosting team invaluable. Support provided a detailed report on why certain log actions were necessary to respond to customer requests, Development prioritized product improvements to reduce privacy risks, and our SaaS team reviewed all logging practices and coordinated with suppliers to ensure a complete response to the data subject access request. The quick and proactive collaboration ensured we could immediately improve our practices and gives confidence that any future issues will also be quickly mitigated.

In summary, we appreciate the constructive feedback from the auditors and remain committed to continuous improvement. Customers can trust TOPdesk is a secure and privacy-conscious solution, and we’ll keep improving our product and services as we complete the final mitigating actions.

Table of contents

Overview of figures, tables and screenshots

Summary

This report is a Data Protection Impact Assessment (DPIA) on the use of TOPdesk for Education (hereinafter: TOPdesk DPIA). This DPIA is written for the Dutch research and education institutions, sometimes abbreviated to ‘institutions’. The first version of this DPIA was published 15 January 2026.

Scope: TOPdesk SaaS

TOPdesk is a cloud-based platform designed for service management, offering a wide range of modules such as Change Management, Incident Management and Asset Management. TOPdesk is used by a wide range of organisations, from businesses to government bodies. In practice, the system is often used to manage company (IT) resources, report incidents and/or as a knowledge base. Within the Dutch education sector, TOPdesk is used by vocational colleges, universities of applied sciences and universities.

This DPIA assesses the risks to the rights and freedoms of employees, students, and other Data Subjects of institutions associated with the use of TOPdesk for a number of predefined use cases:

- TOPdesk as Ticketing system for IT services
- TOPdesk as system for incident management (handling of information security incidents and Personal Data breaches)
- TOPdesk for registration of accidents/inappropriate behaviour in the context of social safety
- TOPdesk within the HR department for the handling of inquiries and issues about integral safety, complaints and confidentiality
- TOPdesk for the Processing of sensitive information of device, incident, application and complaint management

Additionally, risks associated with application- and audit logging and the establishment of authorisation and access rights within TOPdesk by institutions are focus points of this DPIA.

As this is an umbrella DPIA, it does not contain an assessment of the lawfulness of specific Processing Activities, nor risks that are specific to individual institutions. Rather, a more general assessment is made based on the envisioned use of TOPdesk by institutions. Further, optional components (such as a Live Chat functionality and a Feedback Solution) and systems from third party vendors that connect to TOPdesk via an API are out of scope of the DPIA. Institutions wishing to use TOPdesk can use this DPIA as a starting point, but must supplement, expand and/or adapt it based on the specific context in which they intend to use TOPdesk.

Methodology

This DPIA is based on:

- Desk research and legal review on TOPdesk’s documentation, knowledge base, pertinent terms and conditions, contracts and agreements
- Several interviews involving representatives from TOPdesk, staff members of an educational institution that uses TOPdesk and representatives from SURF
- Onsite technical investigation carried out at an educational institution, using a specialised monitoring tool (man-in-the-middle proxy)
- Data Subject Access Requests, filed after technical investigation was performed
- Reviews by TOPdesk and SURF

The role of the representatives of TOPdesk deserves a special mention. TOPdesk has been very transparent, and has proactively fixed several issues, throughout the process. On several occasions, for example when the involvement of Sub-Processors was needed for answering the Data Subject Access Requests, the representatives of TOPdesk made exceptional efforts to obtain information and make additional arrangements.

Outcome: 9 high and 3 low risks
This DPIA has identified nine high risks and three low risks to the rights and freedoms of Data Subjects. These risks are partly due to the way institutions (will likely) use TOPdesk, and partly due to the design of TOPdesk itself. Three of the high risks are linked to the possibility that an institution Processes Special Category Personal Data in TOPdesk; if an institution does not do this, these three risks do not apply. Additionally, risks arise from the optional engagement of (Sub-)Processors by either TOPdesk or an institution.

Measures have been proposed for all risks, including the three low-level risks. Seven of these measures apply to institutions and ten to TOPdesk. Implementing these measures will mitigate all high risks, leaving only low residual risks.

> **Update 12/12/2025:** While the DPIA was being carried out, TOPdesk already implemented several measures to mitigate identified risks. More specifically, TOPdesk has already taken measures for four high risks (#2, 3, 8, 9) and implemented measures for all low risks. One high risk only needs measures from the institution. As such, at the time of writing, four high risks remain. All of these risks have a timeline for implementing the measures.

An overview of all identified risks and proposed measures is presented in the table below. Insofar as TOPdesk has already taken measures or has expressed its intention to take measures, this is reflected in the right-hand column.

Table 1: Overview risks, measures and status

#	Risk	Measures Institution	Measures TOPdesk	Status of TOPdesk measure
1.	Loss of control – lack of policies regulating Personal Data in TOPdesk's log files	None	Create and implement logging Policy describing what kind of Personal Data is logged at each log level.	TOPdesk has created a logging policy which needs to be implemented by all departments. The deadline for this is Q4 2026.

#	Risk	Measures Institution	Measures TOPdesk	Status of TOPdesk measure
2.	Loss of control when contracting based on the TOPdesk template DPA – use of optional Sub-Processors of TOPdesk	Ensure the DPA between the institution and TOPdesk reflects the Sub-Processors that are factually engaged	Define optional Sub-Processors within table on SaaS website.	Since 06-10-2025 TOPdesk's SaaS information page lists which Sub-Processors are optional and informs customers that they can find the applicable Sub-Processors in their Main Agreement. Due to this implemented measure, the risk is now low.
3.	Loss of control – Active subscription required for updates on TOPdesk's Sub-Processors	None	Actively inform all Controllers on changes to Sub-Processors and ask for consent for each change.	On 09-10-2025 TOPdesk adjusted its policy. Now, all registered SaaS Main Contact Persons receive a notification of a new Sub-Processor by default. Due to this implemented measure, the risk is now low.
4.	Loss of control – Transfer of Personal Data via Cloudflare not reflected in DPA	Ensure that the transfer of Personal Data via Cloudflare is properly reflected in the DPA and complies with Chapter V GDPR	Amend the TOPdesk template DPA to reflect the transfer of Personal Data to Cloudflare	This risk is low, so no measures are mandatory, however TOPdesk will implement this measure by Q1 2026.
5.	Loss of control – ex-EEA access requests at Cloudflare			This risk is low, so no measures are mandatory. However TOPdesk will continue to monitor possible disclosures by Cloudflare.

#	Risk	Measures Institution	Measures TOPdesk	Status of TOPdesk measure
6.	Loss of control – transfer of Personal Data via Microsoft			This risk is low, so no measures are mandatory. However TOPdesk will continue to monitor possible disclosures by Microsoft.
7.	Loss of control – Automatic anonymisation fails for third Data Subjects	Implement one of, or a combination of: • A policy to not include Personal Data about third persons in the free text fields of a card • A policy to manually anonymise the fee text fields of a card • A policy to not anonymise but delete cards after their retention period	None	Not applicable
8.	Inability to exercise Data Subject rights – Untimely assistance by Cloudflare and Microsoft	None	Implement a procedure to provide personal data from the logfiles of Cloudflare.	On 17-09-2025 TOPdesk has implemented a procedure for providing personal data from the logfiles of Cloudflare. Due to this measure, the risk is now low.

#	Risk	Measures Institution	Measures TOPdesk	Status of TOPdesk measure
9.	Inability to exercise Data Subject rights – Data invisible for Caller	Implement procedure to include invisible answers in the answers to Data Subject requests.	None	On 18-11-2025 TOPdesk has added the need of implementing this procedure to the best practices in the knowledgebase.
Risks & measures for institutions Processing Special Category Personal Data with TOPdesk				
#	**Risk**	**Measures Institution**	**Measures TOPdesk**	**Status of TOPdesk measure**
10.	Loss of confidentiality & unlawful Further Processing – Use of Special Categories of Personal Data in test or staging environment	Make use of option to run database queries to replace Personal Data from production environment with synthetic data prior to copying the data to a test or staging environment	Offer the possibility to automatically remove the private and contract tab from the cards when transferring production data to a test or staging environment.	TOPdesk has indicated that they are working on implementing this measure. Deadline is Q2 2026. Additionally, on 18-11-2025 TOPdesk has added the need of implementing this procedure to the best practices in the knowledgebase.
11.	Loss of control – Processing Special Category Personal Data in TOPdesk	Perform the proper compliance work prior to Processing Special Category Personal Data in TOPdesk to ensure the institution can rely on one of the exceptions in Article 9(2) GDPR. When Processing Special Category Personal Data in TOPdesk, ensure that this is properly reflected in the DPA with TOPdesk	Create or update a knowledge item for Institutions that provides information and best practices on processing special category data in TOPdesk.	TOPdesk has indicated it expects this measure to be implemented by end of Q4 2025.

#	Risk	Measures Institution	Measures TOPdesk	Status of TOPdesk measure
		Don’t configure (medical) conditions in Attentions, but relevant actions for an operator to take.		
		When registering Special Category Personal Data of a Data Subject, make use of the private tab on the Person card in the Supporting Files module (see §1.2.9).		
12.	Loss of control – insufficient audit logging on Special Categories of data	In absence of TOPdesk’s implementation of additional logging on access and modification of the private tab: Implement audit logging on accessing cards of processes likely to contain Special Categories of data.	Implement additional audit logging: log who opened which card when and add this option to custom log actions	TOPdesk will implement additional logging on access and modification of the private tab on the Person card by default. This is scheduled for Q1 2026.
		After TOPdesk’s implementation of additional logging on access and modification of the private tab: make use of the private tab on Person Cards to Process Special Category Data		

Introduction

This DPIA is commissioned by SURF, the collaborative institution that procures ICT facilities for higher education and research institutions in the Netherlands. The DPIA is performed by Privacy Company in collaboration with stakeholders from SURF and TOPdesk.

Data Protection Impact Assessment

Under the terms of the General Data Protection Regulation (GDPR), an institution is obliged to conduct a Data Protection Impact Assessment (DPIA) when an envisaged Processing of Personal Data constitutes a high risk for the rights and freedoms of Data Subjects. The assessment is intended to shed light on, among other things, the specific Processing Activities, the inherent risks for Data Subjects, and the safeguards applied to mitigate these risks. The purpose of a DPIA is to ensure that any risks attached to the process in question are mapped and assessed, and that adequate safeguards have been implemented to mitigate those risks in such a way that no high risks remain.

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 for example the freedom of expression.

The right to data protection is therefore broader than the right to privacy. Recital 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”*.

This DPIA follows the structure of the DPIA Model as developed for Dutch governmental institutions.

Umbrella DPIA

In GDPR terms SURF is not the Data Controller for the Processing of Personal Data via the use of TOPdesk. The Data Controller is the individual educational institution that decides to use this Software-as-a-Service (SaaS) solution. However, as central negotiator for many cloud services, SURF takes the responsibility to assess the data protection risks for the end Users and to ensure the data Processing complies with the GDPR. Therefore, SURF commissions umbrella DPIAs to assist the educational institutions in selecting a privacy-compliant deployment, and conducting their own DPIAs where necessary. Only the institutions themselves can assess the specific data protection risks, related to the technical privacy settings, nature and volume of the Personal Data they process and vulnerability of the Data Subjects.

Pursuant to article 35 of the GDPR, a DPIA is mandatory if an intended data Processing constitutes a high risk for the Data Subjects whose Personal Data are being processed. 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.[1] If a Processing is not included in this list, an institution 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.[2] As a rule of thumb if a data Processing meets two or more of these criteria a DPIA is required.

It should be noted that whether there is a DPIA obligation in practice depends on the actual Processing operations that a higher education or research institution (hereinafter '(educational) institutions') will carry out using TOPdesk. In the context of this DPIA, it is assumed that there will be high-risk Processing operations that meet the criteria of the Dutch DPA and the EDPB.

The envisioned use of TOPdesk by institutions may involve Processing Activities which are likely to present a high risk according to the Dutch DPA, namely the Processing of health data. This may occur as TOPdesk is intended to be used:

- by institutions for the registration of accidents/inappropriate behaviour in the context of social safety; and
- within the HR department

As such, a DPIA for the envisioned use of TOPdesk by institutions is mandatory based on the Dutch DPA's criteria.

Further, the envisioned use by institutions meets three of the nine criteria of the EDPB meaning a DPIA obligation also applies on that basis:

- Processing of Special Category data or data of a highly personal nature[3]
- large scale Personal Data Processing[4]
- data about vulnerable Data Subjects[5]

This umbrella DPIA is meant to help institutions that have determined that the Processing Activities they (will) perform with the use of TOPdesk mandates a DPIA. However, <u>this document cannot replace the specific risk assessments the different institutions must make themselves</u>.

---

[1] Autoriteit Persoonsgegevens, https://www.autoriteitpersoonsgegevens.nl/documenten/lijst-verplichte-dpia.

[2] European Data Protection Board, https://ec.europa.eu/newsroom/article29/items/611236.

[3] Namely in the context of the registration of accidents/inappropriate behaviour in the context of social safety, and the use of TOPdesk within the HR department.

[4] Within the context of this DPIA, Processing is assumed to be large-scale because, in theory, the Personal Data of all students and/or employees of an institution can be processed in/with TOPdesk throughout their entire period of study/employment. This constitutes large-scale Processing in view of the number of Data Subjects involved and the period during which Personal Data are processed.

[5] Data Subjects whose Personal Data are processed within TOPdesk may qualify as vulnerable Data Subjects. This is especially true for students and employees of institutions because there is an imbalance of power between them and the institution where they are registered/which is their employer.

Scope

TOPdesk is a cloud-based platform designed for service management, offering a wide range of modules such as Change Management, Incident Management and Asset Management.

This DPIA examines the potential impact on Data Subjects of the Processing of Personal Data with the use of the TOPdesk system by educational institutions in the Netherlands. The scope of the DPIA is necessarily broad because each institution is likely to implement and use TOPdesk in a (slightly) different manner. Therefore, this DPIA assesses four use cases of TOPdesk to identify general privacy risks that Data Subjects may face when institutions deploy TOPdesk within an educational/research context. These use cases have been selected as they provide a representative reflection of TOPdesk's intended functionality and typical deployment scenarios within education and research institutions. The table below reflects the scope of this DPIA and outlines the four assumed use cases:

Table 2: TOPdesk use cases within scope of this DPIA.

Use case
TOPdesk as Ticketing system for IT services
TOPdesk as system for incident management (handling of information security incidents and Personal Data breaches)
TOPdesk for registration of accidents/inappropriate behaviour in the context of social safety
TOPdesk within the HR department for the handling of inquiries, integral safety, complaints and confidentiality issues
TOPdesk for the Processing of sensitive information of device-, incident-, application and complaint management

In addition to these use cases, this DPIA also focusses on the Processing Activities inherent to the use of the platform:

Table 3: Additional focus points of this DPIA

Additional focus points
Application and audit logging
The establishment of authorisation and access rights within TOPdesk by institutions.

Outside the scope of this DPIA are:

- The lawfulness of the Processing as required per article 6(1) GDPR: each individual institution must determine this for their specific situation.
- The privacy risks that are specific to individual institutions. Each will likely adapt the platform to their specific needs and organisational context. This creates significant variation in potential Data Processing Activities, purposes, and risk profiles which are not assessed within this DPIA. Each participating institution remains responsible for conducting their own specific risk assessment to evaluate how the general risks identified in this DPIA apply to their particular implementation, taking into account their specific Data Processing Activities, legal obligations, and organisational context. This organisational-specific assessment should complement and build upon the general risk framework established in this DPIA.

- The Ebbot Live Chat, Ebbot AI Chatbot and Insocial Feedback Solutions: these are optional components that are not part of the standard configuration of TOPdesk and that are not part of the standard license and DPA between TOPdesk and SURF.
- TOPdesk can use of the mail servers of the institution. These mail servers send notification messages to users. These mail servers of the institutions should be assessed in a separate DPIA.
- Systems from third party vendors that connect to TOPdesk via an API. These third-party systems should be assessed in a separate DPIA. In part because these APIs are highly configurable so the Data Processing Activities can only be assessed once such an integration is made.

Methodology

The DPIA began with desk-research on TOPdesk's documentation and its knowledge base. This was followed by a series of interviews involving representatives from TOPdesk, staff members of an educational institution that uses TOPdesk, and personnel from SURF. To gain a deeper technical understanding, an onsite investigation was carried out at the educational institution using a specialized monitoring tool — essentially a man-in-the-middle proxy – to trace Personal Data flows and analyse the resulting log files. In parallel, a support request was submitted by the institution where the technical research was performed to obtain assistance from TOPdesk with a Data Subject Access Request. The next phase involved a legal review of the pertinent terms and conditions, contracts, and agreements. Finally, the findings were reviewed by TOPdesk and SURF.

The role of the representatives of TOPdesk deserves a special mention. TOPdesk has been very transparent, and has proactively fixed several issues, throughout the process. On several occasions, for example when the involvement of Sub-Processors was needed for answering the Data Subject Access Requests, the representatives of TOPdesk made exceptional efforts to obtain information and make additional arrangements.

Technical research

Several tests were carried out for this DPIA. A number of scenarios were run through for these tests. For each scenario, both the data visible on the screen and the data exchanged between the browser and the servers were recorded. The tests were designed to cover the use cases mentioned in Table 2 above. Part of the tests is the examination of log files (application logging and audit logging) and audit trails, as well as the structure of authorisations and read permissions in TOPdesk. The script is included in the technical appendix.

Four TOPdesk-accounts were created to perform the technical research. Each was assigned one of the following roles:

- Support
- Security Officer
- School Safety Coordinator
- Supervisor/Administrator

The tests were carried out in the test environment of a Dutch education institution, MBO Utrecht. The accounts were linked to existing employees of Privacy Company. After testing, the institution submitted a support request to TOPdesk for support with Access Requests (ex. art. 15 GDPR) on behalf of the test Users.

During testing, network traffic between the browser and servers was intercepted. This traffic was analysed afterwards. The procedure of the tests and the complete results are included in the technical appendix. Additionally, the log files of TOPdesk as they were available to the educational institution were downloaded and analysed on the presence of Personal Data. Where relevant, the results are presented in the main text.

This report contains the results of the tests and the legal analysis of the findings of the investigation. This report is accompanied by a technical appendix with a detailed description of the test results. This report and the accompanying technical appendix will be published by SURF.

Reader's guide

Certain terms/concepts in this DPIA are capitalised. These terms refer to the definitions as used within either laws and regulations such as the General Data Protection Regulation (e.g.: 'Personal Data' or 'Processor'), or in TOPdesk documentation (e.g.: 'Asset', 'Call', 'Card', 'Operator' and 'User' (or: 'Caller')).

> *Note: throughout the DPIA, and in TOPdesk documentation, the term 'Call' (Dutch: Melding) is often used. This does not refer to a (mobile) phone call. TOPdesk is often referred to as a 'ticketing system' as its main use case involves the creation of 'tickets' to have issues, questions, requests, etc. resolved. These 'tickets' are known as 'Calls' within TOPdesk.*

Further, throughout the DPIA cross-references are made to other sections of the DPIA in blue underlined text. Navigate to the referenced section by holding 'Ctrl' ('Cmd' on iOS) when mouse clicking the text.

The DPIA contains an Annex that provides additional information on each of the TOPdesk modules.

Outline

This Data Protection Impact Assessment assesses the use of TOPdesk by Dutch educational institutions. This DPIA follows the Dutch government DPIA-model. That 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

Part A explains the tested elements of TOPdesk SaaS software. This part starts with a description of the way TOPdesk works, and how the different components and modules interact. This section describes the categories of Personal Data and Data Subjects that may be included in the Processing; the purposes of the data Processing; the different roles of the involved parties; the different interests related to this 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 TOPdesk.

Part B provides an assessment of the lawfulness of the data Processing through TOPdesk. 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. This section provides an analysis of how TOPdesk and it’s Sub-Processors handle requests from Data Subjects 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 specifically 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 TOPdesk or the institutions to mitigate high, medium 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 the data Processing

The first part of the DPIA provides a general description of the Personal Data Processing Activities taking place when using TOPdesk in 6 use cases (the 4 use cases and additional focus points).

1. Description of the system

TOPdesk is a cloud-based, Software-as-a-Service (SaaS) application that provides a wide range of service management solutions. TOPdesk is typically referred to as a 'service management system' (SMS), 'IT management system' or 'ticketing system' used to support internal service provision, the management of IT systems, processes related to Facility Management or Human Resources, and more. In the context of this DPIA, TOPdesk is typically used within higher education or research institution for managing support requests and various operational tasks, answering questions and handling incidents. Further, TOPdesk is used to facilitate reservations for work-/study spaces, managing service level agreements (SLAs) and contracts and can serve as an internal knowledge base.

In TOPdesk, every request, task, question, etc. is known as a 'Call'. Calls are registered as 'Cards' in TOPdesk – essentially digital tickets or notifications (Dutch: meldingen). Within the context of this DPIA, Users include employees or students. Via TOPdesk they can get into contact with Operators, which typically consist of employees of IT teams, service departments, HR, and facilities management.

This DPIA examines the general risks for Data Subjects associated with the Processing of Personal Data as a result of the use of TOPdesk by Dutch education and research institutions. More specifically, the 'Engaged' subscription is examined, which consists of the following modules:

- Incident management
- Problem management
- Supplier management
- Event management
- Space management
- Change management
- Workflow management
- Service Level management
- Self-service portal
- Contract management
- Configuration management
- Knowledge management
- Task management
- Survey management
- Reporting function
- Reservation management
- Visitor registration

These modules can be utilised by institutions for the following use cases:

Table 4: Use cases of TOPdesk within scope of the DPIA, with practical examples

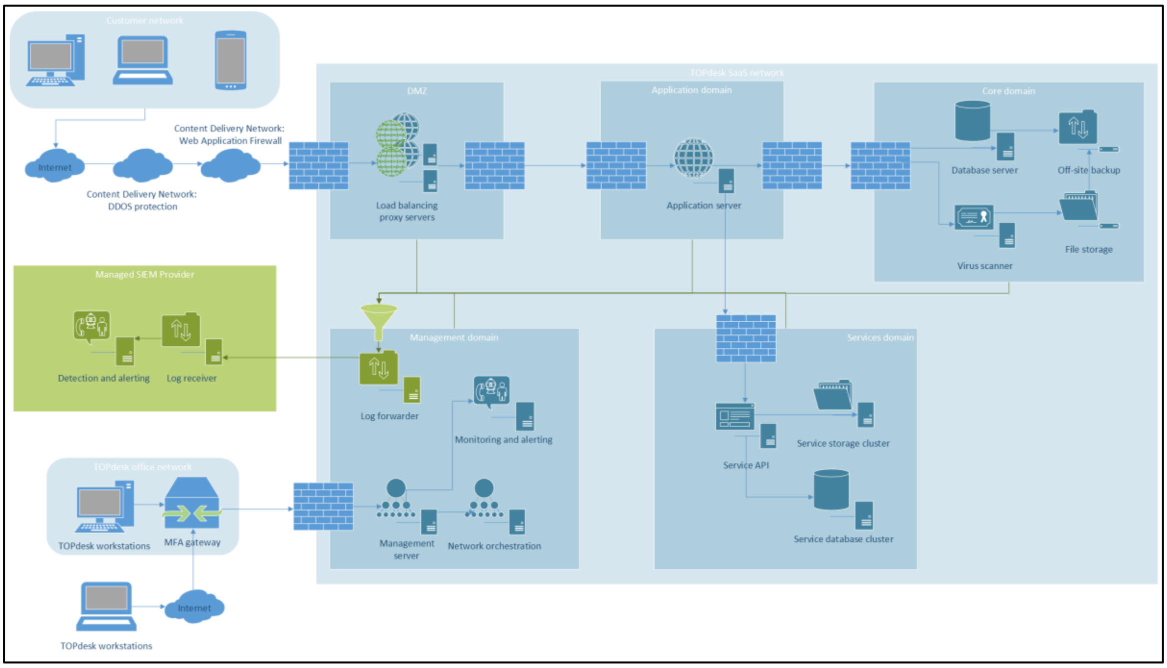
Use case	**Practical example**
TOPdesk as a Ticketing system for IT services	A student/employee encounters a software issue and submits a ticket in TOPdesk. The IT support team receives the ticket, prioritises it, and resolves the issue, keeping the student/employee updated on the progress.
TOPdesk as a system for incident management (handling of information security incidents and Personal Data breaches)	When a data breach occurs, the IT security team logs the incident in TOPdesk. They document the details, track the investigation process, and communicate with affected parties.

TOPdesk for registration of accidents/inappropriate behaviour in the context of social safety/ TOPdesk within the HR department for the handling of inquiries, integral safety, complaints and confidentiality issues	A student/employee reports an incident of harassment through TOPdesk. HR receives the report, investigates the matter, takes action and communicates with the student/employee.
TOPdesk for the Processing of sensitive information of devices, incident, application and complaint management	An institution uses TOPdesk to manage incidents related to sensitive data, such as lost devices or application errors. They log each incident, track resolutions, and communicate with Users.
Application and audit logging	An institution uses TOPdesk to log all User activities within the system, including ticket submissions and changes made to records. This audit trail helps ensure accountability and compliance with internal policies.
The establishment of authorisation and access rights within TOPdesk by institutions.	An institution configures TOPdesk to define User roles and permissions, ensuring that only authorised personnel can access sensitive information or perform specific actions, such as approving requests or managing incidents.

In this first section of Part A, a description of TOPdesk's architecture and the different TOPdesk modules which involve the Processing of Personal Data are provided. The subsequent sections of Part A will refer to this information.

1.1 TOPdesk architecture

Figure 1: Architecture overview TOPdesk SaaS network and DMZ[6]



A TOPdesk User connects to TOPdesk via the internet using a web browser. This connection first passes through a firewall and DDOS protection provided by Cloudflare. This DDOS protection takes place in a data centre located as close as possible to the User. For this filtering on User location, the IP addresses of Users are processed at all locations where Cloudflare has data centres worldwide. The network traffic including the content of the data is not decrypted for this filtering.

After the DDOS Protection, the network traffic is forwarded to a Cloudflare location as close as possible to the data centre location the TOPdesk customer has chosen. In this location Cloudflare runs an application firewall that decrypts the traffic and filters it on known attacks like SQL injections. Unsuspicious traffic is forwarded. Suspicious traffic can, depending on the suspicion, be blocked, or the User can be presented a 'challenge'[7] by Cloudflare. Forwarded traffic is re-encrypted before it is sent to the infrastructure of TOPdesk.

The TOPdesk infrastructure runs on Microsoft Azure cloud. In the TOPdesk infrastructure, the traffic is first filtered by a firewall, then distributed over multiple servers by the load balancer and next it has to pass through firewalls to get to the application servers. The application servers are virtual machines. These hold the main application logic of the TOPdesk application. The storage of these application servers is located in a database cluster and file servers which are accessible for the application servers through another set

---

[6] TOPdesk, https://page.topdesk.com/hubfs/TOPdesk%20SaaS%20Network%20and%20DMZ%202021-09.png <last accessed 01/08/2025>.

[7] Challenges may consist of, for example, an image recognition test. See also: https://www.cloudflare.com/learning/bots/how-captchas-work/ <last accessed 02/09/2025>.

of firewalls. This storage is also scanned for viruses. The storage, database and customer environment configuration are backed up.

TOPdesk is in the process of migrating their application from a monolithic architecture to a services architecture. Some parts of the application have already been split into separate services. These services connect to the main application servers through their own firewall. The services run in docker containers and have their own database instances and file storage.

The infrastructure of TOPdesk also has a management system, which orchestrates the deployment of the servers, databases and containers and manages them. The management system also allows for monitoring and Security Incident and Event Management (SIEM). The SIEM is run by an external third party and monitors system configuration files and the running processes to detect malicious behaviour.

The SIEM processes information on operating system level, not on application level. As a result of that, the SIEM only processes the IP addresses of servers within the TOPdesk SaaS network and information about the system administrators of TOPdesk, but no information about the Users of TOPdesk.

1.2 TOPdesk modules

This paragraph provides a description of the different TOPdesk modules. The described modules are, to a greater or lesser extent, all relevant for the use cases of TOPdesk that are within scope of this DPIA.

1.2.1 Action Management

In TOPdesk's Action Management module, institutions can configure Events that trigger an Action. For example, institutions can configure an Action (e.g. an automated email) that notifies Callers when their Call has been resolved (Event). Events and Actions are incorporated in all processes in TOPdesk and can be set up for basic notifications, such as sending out an email or creating a log entry.

Below, a few specific Actions are further discussed as they are relevant for the assessment of privacy risks in part B of this DPIA. Annex 2 contains two tables that provide more detailed information on all Events and Actions that can be configured.

1.2.1.1 Automated Actions (Action Sequence)

Automated Actions, based on API requests, can be configured to exchange (personal) data between TOPdesk and another application (another TOPdesk environment or a different application/system such as Blackboard or Osiris). This way, integrations with almost any software that has a REST API can be created. These integrations may result in the exchange of (personal) data. The third party providing the other application/system can be an independent Data Controller engaged by an institution (e.g. a government body) or a (Sub-)Processor (e.g. Blackboard or Osiris).

1.2.1.2 Log Actions

Institutions can create a Log Action that is automatically triggered when, for example, changes are made to (certain Fields on) a Card by a User or Operator. The resulting Log

Entry will contain Personal Data of Users and/or Operators, such as names. The specific categories of Personal Data, and whether they include sensitive Personal Data, will depend on the institution's specific log configuration settings. Institutions can use Log Entries for various purposes, such as providing evidence during an audit or supplying information to Data Subjects as part of an Access Request.

1.2.2 Asset Management

Through TOPdesk's Asset Management module, institutions can register their Assets, such as mobile devices and other hardware, but also real estate and specific rooms within buildings. The module provides an overview of all registered Assets. Institutions may create and edit their own template Cards for their Assets, enabling them to determine which information is registered per Asset type. Each Entry Field on an Asset Card is referred to as a Widget. These Widgets may contain Personal Data such as the name of the owner of an Asset or the phone number associated with a mobile phone. Assets can be edited after creation; any changes that are made to an Asset Card are registered in the audit trail.

1.2.2.1 Permissions for Asset Management

Through the Asset Management module, permissions can be assigned to Permission Groups for each Asset type the group manages. Permission Groups are created in the Supporting Files & Property Management module. Specific permissions are required to create, edit, and – most relevant within context of this DPIA – view information (potentially including Personal Data) on an Asset Card.

1.2.3 Self-Service Portal

TOPdesk's Self-Service Portal ('SSP') enables Callers to make use of the services provided by an institution in the Service Catalogue. Annex 2.3 contains screenshots and additional information on the Self-Service Portal.

1.2.3.1 Customising the SSP

Through the Self-Service Portal Designer, institutions can customise the SSP to the needs of their Users. Institutions determine which services are available in the Service Catalogue. Services are grouped by service types and can be offered to person groups, branches and other target groups. For example, the Service Catalogue for the group 'students' might offer a Service to reserve a study space with a computer, while the Service Catalogue for the group 'employees' might offer a Service to reserve a working space or register a visitor. For each available service, the SSP contains a Tile through which it can be requested/used.

Additionally, the SSP landing page provides an overview of current information such as service disruptions and – for managers – requests/Calls waiting for approval. Annex 2.3 contains examples of what a customised Service Catalogue and SSP might look like.

1.2.3.2 Creating Calls & analysing search terms

When a Caller requests to make use of a service through the SSP, a Call is created. Calls are registered under a unique code (e.g. 'C 1604 005') and stored in the Call Management module. When enabled, Callers can monitor the progress of their Call from the SSP, respond to Operators and give feedback when a Call has been handled.

To learn more about topics that are relevant to Users, institutions can analyse the used search terms by downloading an XLS file with an overview of recently used search terms. The used search terms are not related to individual Users.

1.2.4 Call Management module

Within the Call Management module, all incoming Calls (i.e., tickets/notifications or, in Dutch, meldingen)[8] are registered. Calls are (automatically) assigned to an Operator (group) which will process the Call. If the 1st line Operator is unable to resolve the Call, it is escalated to a 2nd line Operator – which can also be an external party such as a supplier. Relevant in the context of this DPIA is that this external party may qualify as an independent/joint Data Controller or (Sub-)Processor for the Personal Data that is shared with them by an institution.

1.2.4.1 Creating a Call

Calls can be created manually or through an API, by Operators and Callers. API's can be used to have people create a Call via external sources such as, for example, the website of an institution or through another environment such as Blackboard or Osiris. Alternatively, a Call can be created by an Operator via an Asset/Location Card.

1.2.4.2 Processing Calls

TOPdesk distinguishes five Actions while Processing Calls:

- Registration - Each Call is registered in TOPdesk as a Card. Registration is the result of an Event (e.g. 'Submit Call') which could be triggered by filling in a form on the SSP, receiving an e-mail or answering a phone call. Information about the Caller who submitted the Call and the means through which the Call was submitted (e.g. SSP, e-mail, etc.) are registered. Additional information can be added, for example when a Caller provides new information about an issue.
- Classification - Before Processing a Call, it should be clear what type of Call it is (i.e. incident notification, request or question), which Service it concerns and other associated information, like a related Asset or location. In classifying a Call, it can be linked to an Asset- or location Card.
- Prioritising – Determine which Call to process first.
- Processing - Performing the required work to resolve the Call.
- Closing - Once all required work has been performed and the Caller is satisfied with the result, the Call may be closed.

When responding to a Call, Operators can choose to have their answer be 'invisible to a Caller' which allows for internal communication relating to the Call.

When a Call is created to report an incident, and a similar incident has been reported before, a Problem Card can also be generated in addition to the Call Card. More on Problem Cards in the section on Problem Management.

From a (resolved) Call, a Knowledge Item can be created to share best practices, lessons learned, etc. In doing so, the entire history of a Call is used to create the Knowledge Item. Entry fields of the Call can be edited/emptied, e.g. to remove Personal Data, before publishing the Knowledge Item through the Knowledge Management module. When

---

[8] Note: as mentioned previously, within TOPdesk a 'Call' does not refer to a (mobile) phone Call, but to the notification/ticket that is created to make a request, report an incident, ask a question, etc.

creating a Knowledge Item from a Call, information about the Caller, Operator, institution, etc. is not used.

1.2.5 Contract Management and SLM

TOPdesk's Contract management and SLM (Service Level Management) module serves two purposes:

- Managing service contracts for (internal) clients
- Keeping track of (contracts signed with) suppliers

The latter is most relevant in context of this DPIA: the Contract Management and SLM module could be used by institutions to help manage Data Processing Agreements and/or Joint Controller Agreements with (Sub-)Processors and joint controllers, facilitating compliance with GDPR accountability requirements[9].

1.2.6 Operations Management

Operational activities, such as maintenance, cleaning and catering can be scheduled in the Operations management module and their progress can be tracked. Operational activities are assigned to individual Operators or Operator Groups.

1.2.7 Problem Management

The Problem Management module enables institutions to process (large) groups of Calls more efficiently. Calls (likely) caused by the same problem, can be collected in a Problem Card in the Problem Management module. The Problem then becomes a Known Error, for which a workaround can be defined. Problem Cards and Known Error Cards can, to a certain extent, be customised to tailor to an institution's needs. Fields can be added, and certain fields can be made mandatory.

1.2.8 Change Management

TOPdesk's Change Management module can be used to process Requests for Change ('RfCs') within an institution. Examples of changes range from a relatively small Change, such as the addition of an extra functionality to an application or requesting a hardware device, to larger Changes such as the replacing/addition of a mail server. Another example may be the on-boarding of a new employee. In this case, many departments must process Changes, such as setting up accounts (e.g., IT), getting the new employee on the payroll (e.g., HR) and making sure there is a laptop available (e.g., Facility Management). As such, RfCs typically include the Processing of Personal Data.

When filing an RfC, a Card is created and certain information about the request must be provided by the Caller. Alternatively, (P)RfCs[10] can be created from a Call, a Problem or from the Caller Card.

Annex 2.5 contains a flowchart, with an explanation, describing the procedure underlying the Change Management module in more detail and an overview of the Operator roles relevant within the context of Change Management.

---

[9] Article 5(2) GDPR.

[10] PRfC stand for a Preliminary Request for Change.

1.2.9 Supporting Files & Property Management

The Supporting Files module contains the basic data that enables TOPdesk to support an institution's processes and is therefore relevant for all envisioned use cases assessed within this DPIA. Basic data of the institution that will use TOPdesk, and any external parties (such as suppliers), must be registered to be able to perform the institution's processes via TOPdesk. The basic data typically includes Personal Data of registered Operators and Users. On the Person card in the Supporting Files module there is a Private tab that can be used to register, for example, Special Category or sensitive Personal Data such as health information or national identification numbers (Burgerservicenummer). Separate permission groups can be granted access to the Private Tab, allowing institutions to limit visibility of such sensitive Personal Data on a need-to-know basis.

1.2.9.1 Managing external relations

As stated, details of external institutions can be registered in the Supporting Files module, such as details of suppliers and possibly Personal Data of the employees of that supplier. This enables the (direct) placing of orders, submitting service requests or managing contracts in TOPdesk.

1.2.10 Knowledge Management

TOPdesk contains a Knowledge Base which can provide relevant information for the creation and Processing of Calls, (P)RfCs, etc. The Knowledge Base can be used:

- As an encyclopaedia with internal information for Operators
- As an FAQ (Frequently Asked Questions) for Callers in the Self-Service Portal
- For news items on the Homepage for both Operators and Callers

The Knowledge Base is integrated with the Call- and Problem Management Modules so information from a knowledge item can be used in a Call or Problem. Alternatively, a knowledge item can be created from a Call or Problem. As such, this Module is relevant for all envisioned use cases by institutions. Before creating a Knowledge Item from a Call or Problem, any Personal Data contained therein is removed/anonymised and TOPdesk forces the knowledge item to be reviewed manually before publishing it.

1.2.11 Reservations Management

In the Reservations Management module, an institution can configure locations, Assets and services which can be reserved by Operators and Callers. Students, for example, might reserve a study space through this Module. The Module can be configured to automatically approve or decline reservations (based on availability) or require prior authorisation of an Operator.

Note: when trying to make a reservation, Callers will only see available Assets. It is not possible to see reserved Assets, and/or Personal Data of the Data Subject that has reserved the Asset.

1.2.12 Visitor Registration

The Visitor Registration module facilitates the tracking and managing of all visitor-related processes: preparing for visitors, registering them, checking them in and out, monitoring the visit and, ultimately, deleting the visitor's Personal Data after a set length of time.

A Data Subject visiting an institution will be registered as a Visitor, which is a separate role within TOPdesk. As it is a different role, different rules can be applied to the Personal Data of a Visitor such as different (e.g., shorter) retention periods.

1.2.13 Responsible data management

Under the banner of 'Responsible data management', TOPdesk offers several privacy features. Most notably are features related to anonymisation and data removal. Further, TOPdesk also offers the possibility to use synthetic data for test environments.

During setup of a TOPdesk environment, Administrators are notified of these settings. In addition, a Widget has recently been introduced to remind Administrators of the settings. This Widget is a relatively new feature in TOPdesk and will be expanded in the future.

1.2.13.1 Anonymisation and data removal

With the anonymisation feature for Callers and Operators, Personal Data on Caller- and Operator Cards, as well as on Cards that are linked to them (e.g. an Asset Card), can be anonymised manually or automatically after a set time. Only Operators with administrative rights can set anonymisation rules within TOPdesk. Automatic anonymisation applies to Callers who have been archived for a custom period, to be determined by the institution. The process of checking archived Callers and anonymising them when the custom period has been reached is performed daily.

When anonymising a Person or Operator Card, data from all fields that might contain Personal Data is used to find Personal Data in linked Cards and remove it automatically. All found Personal Data is replaced with *****. In addition to this, attached e-mails are removed, log entries are anonymised and hyperlinks containing 'mailto;' are removed. When all linked Cards are anonymised, the Person or Operator Card itself is anonymised to complete the process.

For the Card types 'Call', 'Problem', 'Change', 'Change activity', 'Visitor', 'Reservation', and 'Event', two options are available:
- Anonymise: Personal Data is replaced by '*****'
- Delete: fields are deleted

When anonymising an Operator Card, TOPdesk modifies the Card as well as the Cards that are linked to the anonymised Operator. TOPdesk anonymises name(s) (first- and last name, initial(s) and infix(es)) and e-mail address of the Operator, log entries and hyperlinks containing 'mailto' on the following Card types linked to the anonymised Operator:

- Changes and Change templates
- Change activities and Change activity templates
- Calls
- Problems, Partial Problems and Known Errors

Additionally, irrelevant Card content can be deleted after a chosen period. It removes the following information from closed Cards: request, action, brief description and attached emails. Furthermore, Personal Data of unregistered Callers in the Caller block is anonymised. Other Personal Data of Callers will remain unchanged and can be removed using the anonymise persons functionality.

Annex 2.6 contains two screenshots reflecting an example of an anonymisation request made by a Caller (Screenshot 6) and the effect once such a request is processed (Screenshot 7).

1.2.13.2 Synthetic data

Institutions setting up a test or staging environment, can use either a copy of their production environment or a default set of synthetic data that is available on request at TOPdesk. The synthetic data is not tailored for the custom processes the organisation has defined and therefore has limited use. When using a copy of production data, institutions can choose to anonymise unnecessary information in the database copy to reduce the amount of Personal Data in the test environment. Another option is that the institution creates their own set of database queries to generate synthetic data and contacts TOPdesk to run them, but creating these queries is a relatively labour-intensive process.

On-premise customers of TOPdesk can create Service Accounts for different environments (Acceptance, Production, etc.), as described in Table 5 below. TOPdesk recommends the creation of separate Service Accounts to prevent production data from being processed in an acceptance environment, and vice versa. When using TOPdesk SaaS, TOPdesk automatically creates separate Service Accounts for each environment to ensure data separation.

1.2.14 Setting up TOPdesk

The final paragraphs of this Section address additional information regarding the setup of a TOPdesk environment by/for an institution. This is relevant to this DPIA since it involves the Processing of Personal Data.

1.2.14.1 Roles within TOPdesk

When setting up TOPdesk, there is a degree of configurability allowing for the creation of different roles. The assigned role determines the authorisation and access rights within TOPdesk and, as such, determines which Actions a Caller or Operator may perform. The table below provides a non-exhaustive overview of some of the roles that can be assigned to an Operator in TOPdesk:

Table 5 Overview of roles that can be assigned within TOPdesk

Role	Description	Actions
Caller	Students, employees and external persons with access to one or more TOPdesk functionalities.	• Read • Write • Create • Edit • Delete
Operator	User that handles Calls submitted by Callers.	• Read • Write • Create • Edit • Delete
Service Account	Per TOPdesk environment (e.g. Acceptance and Production environments) a Service Account can be created. Service Accounts can perform automated	• Read • Import

	Actions such as importing emails from a mail server or adding information of Callers through a connection with an Active Directory or CRM.	
Problem Manager	Coordinator of a Problem Card	• Read • Write • Create • Edit • Delete
Problem Operator	Operator assigned to a Problem Card	• Read • Write • Create • Edit • Delete
Visitor	External visitors of an institution	N/A

When creating a new Operator, the settings from an existing Operator can be copied and assigned to a new Operator. This is useful if the new Operator will perform the exact same tasks as the existing Operator and thus requires the exact same settings and permissions.

1.2.14.2 Authorisation management

Regarding authorisation management, institutions have the option to configure authorisations for different types of Personal Data. HR-related Personal Data can, for instance, be made less accessible than IT-related Personal Data by configuring access rights to such data differently. Using this feature, access to integrity tickets can, for example, be restricted to a small group of HR employees, while access to IT-tickets can be made available to the entire IT department. This allows for the consideration of the sensitivities associated with different types of Personal Data. The authorisations are determined by the Role that has been assigned to a User or Operator. To configure different access rights for different types of (Personal) data (on a single Card), institutions will need to create different Roles and assign the necessary authorisations. Further, institutions can apply Filters to further restrict access to Personal Data. For example, a Filter can specify that a certain operator group may only see certain values in drop-down lists.

1.2.14.3 Attentions

When creating a Caller, an ‘Attention’ can be added to the Caller and Operator profiles. These Attentions can be used to provide additional information about the Caller. It can be used, for example, to indicate that a Caller is hard of hearing or visually impaired, blind or deaf, mobility impaired, etc. This information can be useful when responding to a Call created by the Caller. If someone is hard of hearing, the Operator knows that communication via telephone is not preferred; if someone is visually impaired, the Operator knows that it would be better to Call the User. Attentions can be configured by the institutions themselves.

1.2.15 Imports & external connections

TOPdesk has functionalities to import data, like Users, Operators, suppliers or Assets, from other sources such as an Active Directory or CRM system. The authorisations and roles assigned to a User or Operator in that other source are not (automatically) imported to TOPdesk. Authorisations can be assigned implicitly when importing Users if the department or location is also imported, and if an institution’s Self-Service Portal is configured so that a

User's department or location determines which services in the Self-Service Portal they can access.

Furthermore, TOPdesk has functionalities to involve external parties in the Processing of Calls. On top of that it is also possible to integrate (content from) external web sources within the User interface of TOPdesk. These integrations are referred to as 'web integrations'. These features are discussed below.

1.2.15.1 Imports

Institutions must import various data into their TOPdesk environment(s) and database(s). This can be done through:

A. Standard imports which are executed manually and mainly used to import information about branches, persons, hard- and software.
B. Customized imports, based on customized scripts created with assistance from TOPdesk. This function can also be used to execute imports automatically for a set period (e.g. weekly).
C. Import wizard: to import data for the Asset Management and Support Files modules, the import wizard is to be used. Using the wizard, Assets, persons, branches and locations can be imported from files, databases or, for example, Microsoft Entra ID, Active Directory or a CRM system. These imports can be executed manually or automatically.

1.2.15.2 Calls – sharing/escalating

There are several options for sharing Calls with an external party. The most common option is to send an email through the institution's mail provider or TOPdesk's SaaS mail server. An API connection with an external system is also possible.

Alternatively, there is an option to connect two TOPdesk environments. Which Personal Data the external party processes, depends on how the connection is set up. Connections are always set up by the application administrator or a TOPdesk consultant. In the most common options, the supplier does not have access to the TOPdesk environment itself and only sees the information that is shared with them. If data is sent to a supplier, this is clearly reflected in the TOPdesk logs.

Additionally, depending on the TOPdesk functionalities an institution is going to use, TOPdesk needs access to the mail server of an institution to import email messages. These access rights can be granted to a Service Account which can then automatically import information and/or email messages.

1.2.15.3 Web integrations (Web Widgets)

When setting up a TOPdesk environment, institutions have the option to create integrations with external web content which can then be displayed on the home page or in an Asset Card as a 'Web Widget'. Web Widgets are not enabled by default. When enabled, TOPdesk will open the specified URL and display the result. There is no way to roll out Web Widgets centrally, so they must be set up by the Administrator or an Operator.

Such integrations (may) lead to the sharing of Personal Data from the TOPdesk environment with a third party, such as Google (in the case of an integrated YouTube video). See further: §1.3 Cookies and §1.4 Hosts and third-party connections.

1.3 Cookies

TOPdesk always places the following cookies:

Table 6: Cookies always placed by TOPdesk

Name cookie	Type of cookie	Purpose
JSESSIONID_PUBLIC	Functional	First party session cookie. Keeps track of the User session. Deleted once the browser window is closed.
authsession	Functional	First party session cookie. Keeps track of the authentication of the session. Gets deleted once the browser window is closed.
topdeskidpforwardcacheid	Functional	Cookie used when authenticating a User. It contains a unique User ID ('uuid'). On the server side, the uuid is associated with the URL the User wanted to visit prior to authentication. After authentication the User is redirected to that URL. Once redirected, the value of the cookie is cleared. The cookie gets deleted after 15 minutes.

When performing the test scenarios at MBO Utrecht, several actions lead to the placing of additional cookies:

- The administrators of MBO Utrecht (test site) created a Web Integration in the Asset Management module. This Web Integration showed a YouTube video with some instructions on a migration. By integrating this video, additional cookies were placed.
- When accessing the status page of TOPdesk[11] from the admin site, the browser was referred to reCaptcha to check if the traffic was not part of an automated attack (see: §1.1 TOPdesk architecture). reCaptcha also set a cookie. During these test runs, the following non-standard cookies were set:

Table 7: Observed non-standard cookies

Host	Cookie name	Type of cookie	Purpose
mboutrecht-test.topdesk.net	*@topdesk/topdesk-app/principal-hash*	Functional	First party session cooking, keeps track of the navigation at the admin site.
	JSESSIONID_ROOT	Functional	First party session cookie. Keeps track of the User session, gets deleted once the browser window is closed.

---

[11] TOPdesk, https://status.topdesk.com/

	JSESSIONID_SECURE	Functional	First party session cookie. Keeps track of the User session, gets deleted once the browser window is closed.
	authsession	Functional	See Table 6: Cookies always placed by TOPdesk
	mango_window_size	Functional	First party session cookie, contains the screen size for opening pop-up windows.
	topdeskidpforwardcacheid	Functional	See Table 6: Cookies always placed by TOPdesk
www.youtube.com	*PREF*	Functional	Storage of unknown property, does not contain an ID. Gets deleted when the browser window is closed.
	VISITOR_INFO1_LIVE	Tracking	Contains a string that might function as an ID, gets deleted after 6 months. Keeps track of User profile on YouTube.
	VISITOR_PRIVACY_METADATA	Tracking	Contains a string that might function as an ID, gets deleted after 6 months. It keeps track of the privacy settings of the User, exact content and connected Processing is unknown.
	YSC	Functional	Session cookie
	__Secure-ROLLOUT_TOKEN	Tracking	Contains a string that might function as an ID, gets deleted after 6 months. It keeps track of the roll-out and testing of new functionality of YouTube, exact content and connected Processing is unknown.
www.recaptcha.net	*_GRECAPTCHA*	Tracking	Contains a string that might function as an ID, gets deleted after 6 months. Exact content and connected Processing are unknown.

1.4 Hosts and third-party connections

By default, TOPdesk only connects to the host of the instance of the application: *[instance-name].topdesk.net*. During testing, two exceptions to this default were found:

- The inclusion of a YouTube clip as a web integration resulted in traffic to the following hosts:
    - www.youtube.com
    - i.ytimg.com
    - fonts.gstatic.com
    - www.google.com
    - i.ytimg.com
    - jnn-pa.googleapis.com
    - yt3.ggpht.com
    - rr4---sn-5hnekn7l.googlevideo.com
- Clicking on the link to the status page of TOPdesk resulted in the browser being referred to reCaptcha to check if the traffic was not part of an automated attack (see: 1.1 TOPdesk architecture), which in its turn resulted in traffic to the following hosts:

- dka575ofm4ao0.cloudfront.net
- www.recaptcha.net
- cdnjs.cloudflare.com
- status.topdesk.com
- www.gstatic.com
- atlassian-cookies--categories.us-east-1.prod.public.atl-paas.net
- dka575ofm4ao0.cloudfront.net
- fonts.gstatic.com
- www.gstatic.com

Furthermore, institutions can choose to enable Google Analytics to perform analyses on the use of their TOPdesk environment. During testing, the browser performed requests to /tas/api/sspAnalytics/googleAnalyticsInfo at the TOPdesk site. Because Google Analytics was not enabled in the test environment, these requests were answered with a ‘HTTP 404 – page not found’ response. When enabled, the use of Google Analytics leads to the sharing of Personal Data of Operators and Callers with Google. Which Personal Data this concerns, depends on the configuration of Google Analytics by an institution. TOPdesk offers guidance on the most privacy friendly configuration of Google Analytics.[12] If this guidance is followed, device type, browser used and the visited TOPdesk page(s) are processed with the Google Analytics cookie. When enabled, the entire SSP is analysed by Google. Alternative analytical cookies, such as Matomo, are currently not supported by TOPdesk.

1.5 Hosting

TOPdesk currently offers multiple hosting locations across the world, including multiple European locations. Institutions can choose where their environment is hosted and can verify this location via TOPdesk’s customer service portal. To prevent cross-border Personal Data transfers as much as possible, institutions should select a hosting location within the European Economic Area (‘EEA’). Within this DPIA it is assumed that institutions will select the hosting location in this region, most likely the Netherlands. Personal Data may sometimes be moved to a different virtual hosting location within the same physical data centre. However, Personal Data is never moved to another hosting region (e.g. outside the EEA) without prior, explicit written consent of a mandated person within an institution.

TOPdesk makes use of Microsoft Azure’s hosting services, to which end a Data Processing Agreement has been concluded1.10. TOPdesk uses the following services from Azure:

- Virtual Networking (Infrastructure as a Service)
- Virtual Machines
- Kubernetes containers
- Databases
- Azure Defender (cloud)
- Azure Key Vault

Insofar Personal Data is processed by Microsoft on behalf of TOPdesk, these Processing Activities are covered by the Data Processing Agreement between TOPdesk and Microsoft.[13]

---

[12] TOPdesk, Knowledge Item 11726.

[13] Microsoft Products and Services Data Protection Addendum Apr. 2025, Section ‘Scope’, p. 7-8, https://www.microsoft.com/licensing/docs/documents/download/MicrosoftProductandServicesDPA(WW)(English)(April2025)(CR).docx <last accessed 03/09/2025.

1.6 Back-ups

Back-up procedures aim to ensure that institutions can continue to operate if data becomes unreachable. TOPdesk has the following back-up facilities:

- Continuous database transaction logs ensure data recovery from any point in time for the past 35 days if a disaster should occur.
- Daily off-site attachment back-ups ensure availability of uploaded documents, even in case of a data centre failure.
- Institutions can also store a local copy of their database, by making an export using My TOPdesk, and download attachments directly from their TOPdesk environment. The file download can be set up via a WebDAV file transfer connection.

Storage of back-ups takes place in a different location than where the data is hosted. The back-up location for the hosting location in the Netherlands, for example, is Ireland and vice versa.[14]

When a TOPdesk environment is deleted, a back-up of the deleted environment is stored for 75 days. This back-up is only accessible by TOPdesk (employees).

1.7 Security

1.7.1 TOPdesk's security measures

TOPdesk has an Information Security Management System (ISMS). At the time of writing this DPIA, TOPdesk is pursuing ISO 27001 certification for its ISMS and aims to achieve full accreditation by the end of 2025.

The scope of the certification covers the delivery and support of TOPdesk SaaS services which includes:

- Providing the selected TOPdesk software over standard Internet connectivity; and
- Maintenance, monitoring, providing disaster recovery coverage and updating the TOPdesk software and hosting components.

The scope of the certification does not cover the services provided by TOPdesk's Sub-Processors, namely:

- The housing and hosting services provided by Microsoft Azure.[15]
- Traffic routing, managing of SSL certificates and additional security services provided by Cloudflare.
- The message bus provided by 84 Codes AB (CloudAMQP).
- The Live chat and AI Chatbot integration provided by Hello Ebbot AB.
- Feedback solutions provided by Insocial.

---

[14] See: https://page.topdesk.com/saas-information#servicesetupanddesign <last accessed 14-05-2025>.

[15] NB: The housing and hosting services provided by LeaseWeb are not in scope of the certification either. However, as the institutions that will be using TOPdesk are all located within the European Union (i.e., the Netherlands), housing and hosting services will be provided by Microsoft Azure only – not by LeaseWeb. See: 'Hosting Locations', https://page.topdesk.com/saas-information#encryption <last accessed 11-07-2025>.

TOPdesk is SOC2 certified. The controls referring to TOPdesk as Data Controller are out of scope of the SOC2 audit, because they are not applicable according to the audit. In the context of this DPIA, the SOC2 audit assumes that TOPdesk has established appropriate Data Processing Agreements (hereinafter: ‘DPA’s’) with its Sub-Processors, ensuring that the desired level of data security for Personal Data is upheld by these Sub-Processors.

For completeness, a brief overview of the security measures and their adequacy on the part of the Sub-Processors is provided in §1.7.2 below. Additionally, TOPdesk provides the following assurance on its website: “TOPdesk has Data Processing Agreements with all used data centres. Data centre Operators are not allowed to handle customer data, and control procedures are in place. The effectiveness of these procedures is regularly audited, and TOPdesk reviews the audit results.”[16]

Furthermore, the scope of the certification does not cover:
- The software development process of TOPdesk software components.
- Consultancy services.
- Services provided to non-SaaS (on premises) customers.
- Internal organisational processes and office automation of TOPdesk as long as they have no direct link to or impact on the SaaS services.

Annex 2 contains a complete overview of the security measures implemented by TOPdesk.

1.7.2 Security measures implemented by/through TOPdesk’s Sub-Processors

1.7.2.1 Cloudflare: DDoS protection and Web Application Firewall

All traffic to TOPdesk environments is routed via Cloudflare. Cloudflare first checks the IP address and metadata (OS, browser version) for known attack patterns and displays a challenge for high-risk traffic. In exceptional cases, a decision is made to block the traffic based on this data (DDoS protection). These actions are centrally logged in the US for 7 days (standard) up to a maximum of 1 year (exceptions).

After the DDoS protection, Cloudflare routes the traffic to a Cloudflare data centre closest to the TOPdesk data centre (always in the same country)[17], the traffic is decrypted by Cloudflare, and the request is checked for known attack patterns (Web Application Firewall). Malicious requests are blocked, and the remaining requests are re-encrypted and forwarded to TOPdesk. Cloudflare therefore only has access to traffic to TOPdesk and not to the data stored in the TOPdesk environment. Because the content of the traffic contains session unique IDs, Cloudflare can relate the traffic to a specific customer.

Cloudflare's internal processes are ISO27701 certified, which indicates that the procedures for protecting customer privacy are in line with best practices. TOPdesk annually reviews the latest audit reports from its SaaS suppliers.

1.7.2.2 Microsoft Azure

All TOPdesk’s Azure hosting locations use encrypted disks, for customer files, database back-ups, and TOPdesk databases. Database encryption has been enabled from the

---

[16] ‘Encryption’, https://page.topdesk.com/saas-information#encryption, <last accessed 11-07-2025>.

[17] In each country where a TOPdesk server is active, there is also a Cloudflare server active.

beginning by default on all hosting locations. The encryption keys are managed by TOPdesk using Microsoft Azure's Cloud Key Vault.

TOPdesk and Microsoft Azure aim to ensure that all disks that have contained unencrypted customer data will be overwritten using Darik's Boot and Nuke (DBAN) before reuse, or the disk will be destroyed to make future use impossible. Data is distributed over multiple disk drives. This aims to ensure that an error on a disk does not cause loss of data and that a stolen disk contains only fragments of files and readable data.

1.8 Support by TOPdesk

TOPdesk employees provide support to institutions in connection with the use of the system. In principle, support can be provided by employees from any of the various TOPdesk branches, including branches outside the EEA. TOPdesk uses two distinct systems for providing support:

1. Regular support (ticket handling via My TOPdesk): Customers can submit support tickets through My TOPdesk. This process does not require access to the customer's TOPdesk environment, and support can be provided from any TOPdesk branch. EEA-based customers can opt out of having their support tickets handled outside the EEA. This opt-out can be requested via a form on My TOPdesk. This setting is independent of the authentication and region settings used to manage login access for TOPdesk's Support staff.
2. Environment access by TOPdesk support (opt-in per region): This option refers to situations where a TOPdesk Support employee accesses the customer's environment directly. Such access is only possible if the customer has explicitly opted in for the relevant region. These region-based settings determine from which geographical locations support access by TOPdesk is permitted. TOPdesk support personnel who have completed training and received a certificate of good conduct can log in via their personal account. If a TOPdesk support employee accesses an institution's environment directly, the access logs will show who logged in and when.

The database always remains stored at the chosen location. It will only be stored elsewhere with the explicit written permission of a mandated person within an institution. Access to the servers is reserved for TOPdesk SaaS administrators. Other TOPdesk colleagues can never access them. Data must therefore always be requested from the SaaS environment using the above processes.

1.9 Log files

TOPdesk has several types of logs that are retained for hosting SaaS environments:

- TOPdesk application access logs
- TOPdesk application logs
- TOPdesk service logs
- SaaS hosting server logs
- Product usage metrics/metadata[18]
- (Custom) audit trail logs within the product

To the extent that Personal Data is processed as part of these forms of logging, they are discussed further below.

---

[18] No Personal Data is processed as part of this form of logging.

1.9.1 TOPdesk application access logs

The application access logs contain all log-in attempts in an institution's TOPdesk environment. This information is kept for 6 months and is available for TOPdesk Support and for Operators with the permission *'Webdav \ access logs'* via a WebDAV (file transfer) connection to an institution's TOPdesk environment. The access logs contain login names (e.g. 'ENBT2', 'SEOG', etc.) and IP addresses which both typically qualify as Personal Data. Administrators of the institution can download, and determine who can download, these logs.

Institutions can choose to download the access logs and link them to their own Intrusion Detection System. In cases where an institution has set up TOPdesk to use Single Sign On (SSO), the authentication logs created and retained by TOPdesk are unnecessary as all logins can already be reviewed via the institution's own Identity Provider.

1.9.2 TOPdesk application logs

Application logs contain all actions and troubleshooting information regarding an institution's TOPdesk environment. This information may include Personal Data such as login names, IP addresses, email addresses, email topics, database queries and other information used to troubleshoot problems. It is stored for a short period (no longer than 10 days) and is available for TOPdesk Support to troubleshoot Calls. Administrators of the institution can download these logs.

As part of this DPIA, the researchers extensively analysed the application logs and checked for the presence of Personal Data linked to usernames and IP addresses. In general, the logs follow industry standards and contain only limited amounts of Personal Data. However, some inconsistencies were found. For example, the database query logs contained the full query with all parameters in the logs in some cases, while in other cases only the field names of the parameters were logged. At the same time, the queries containing the parameters were logged at a less verbose log level than the queries with only the field names. When asked about this, TOPdesk indicated that they have a general policy to restrict storing Personal Data in logs to what is necessary. However, TOPdesk does not have specific policies on Personal Data within the different log levels. By default, logging is executed at the debug log level, but this can be adjusted for individual environments as needed. TOPdesk uses one more verbose log level than debug (trace) and three less verbose log levels.

TOPdesk support can only access the application logs after the institution files a support request. The log level of 'debug' is necessary to provide the support with enough information to troubleshoot issues.

1.9.3 Service logs

The TOPdesk service logs contain information on the shared service architecture of TOPdesk. These services are deployed separately from the main TOPdesk product and provide additional functionality. Examples of services are:

- A system to ensure concurrent import runs do not cause a high database load
- An integration to upload relevant log files to bug reports submitted via My TOPdesk
- Tools to support the generation of barcode labels and PDF-files within the TOPdesk product

In principle, logs for these services only contain ID's referring to Cards in TOPdesk, they do not directly contain Personal Data. However, the service logs also contain a unique User ID (32 characters) which qualifies as Personal Data; if someone (e.g. an Operator) has access to the complete TOPdesk environment/database, this unique User ID can be used to identify individual TOPdesk Users. Service logs are typically retained for 30 days, with a maximum of 90 days.

1.9.4 TOPdesk SaaS hosting server logs

The SaaS hosting server logs provide insight into the operational status and performance of the SaaS hosting servers (i.e. the underlying infrastructure that supports TOPdesk). Most notable in the context of this DPIA is that these logs provide information about incoming and outgoing network traffic and, thus, contain IP addresses which may qualify as Personal Data.

1.9.5 (Custom) audit trail logs within the product

Next to these 'standard' logs, institutions can also define an audit trail (with log entries) within their own TOPdesk environment. For several fields on Cards, an institution can determine if TOPdesk should log who changed them and when. Additionally, institutions may create custom audit trails that are triggered at predefined times.[19]

Audit trail entries are stored on the Card for which the audit trail is set. There are no separate access controls for audit trail log entries. Everyone that can access a Card within a TOPdesk environment can view the log entries of that Card. Audit trail entries cannot be edited. These logs are intended to permanently store information for later audits. To protect the Personal Data of Data Subjects working in TOPdesk, audit trail entries are anonymised when the linked person or Operator is anonymised.

1.10 Contractual structure between SURF, institutions & TOPdesk

In 2021, a group of thirty of SURF's members, SURF and TOPdesk entered into a Framework Agreement entitled "Service Management Software". Following the Framework Agreement, institutions had the chance to enter into one or more Further Agreements. Most notable within the context of this DPIA are the Data Processing Agreements. Institutions had the option to either make use of the SURF template Data Processing Agreement (Version 3.0), their own template Data Processing Agreement or the template Data Processing Agreement provided by TOPdesk.

Within context of this DPIA, 2 of these templates are assessed[20]:

1. The SURF template Data Processing Agreement (v3, 2019) – specifically the DPA concluded between MBO Utrecht (the institution where the technical tests were performed) and TOPdesk
2. TOPdesk's template Data Processing Agreement (v.2025)[21]

---

[19] See: TOPdesk, 'Setting up a log action', <https://docs.topdesk.com/VA2023R2/en/setting-up-a-log-action.html> last accessed 25-07-2025

[20] Within this DPIA, it is assumed that institutions will make use of the SURF template DPA. However, as institutions also have the choice to use TOPdesk's own template DPA, this is also assessed to identify any risks therein. Institution specific template DPA's are not assessed as part of this DPIA.

[21] Institution specific template DPA's are not assessed within scope of this DPIA.

Both template DPAs contain all elements required by art. 28.3 GDPR. The table below identifies notable differences between the DPAs.

Table 8: Notable differences between the two different DPA templates

Element in DPA	SURF template DPA concluded between MBO Utrecht and TOPdesk	TOPdesk template DPA
Specification of Processing (Annex)	• The specification of Processing Activities does not mention Processing of Personal Data in the context of logging. • The annex specifies the relevant Sub-Processors, a number of optional Sub-Processors (e.g. Hello Ebbot AB and Insocial) are not listed as engaged Sub-Processors	• The specification of Processing Activities explicitly mentions Processing of Personal Data in the context of logging. • The annex specifies, in addition to the SURF template DPA, that TOPdesk's IT/Development Security Department has access to Personal Data of the institution. • The annex does not specify which Sub-Processors are used to provide the services. Rather, a dynamic/non-static URL to a TOPdesk webpage which provides an overview of possible Sub-Processors, including optional Sub-Processors, is provided.
Special Category Personal Data (art. 9 GDPR)	Does not preclude large scale Processing of Special Category Personal Data by an institution.	Explicitly mentioned that software is not designed or intended to process, at large scale, Special Category Personal Data.
Sub-Processors	• TOPdesk must inform institutions 3 months prior to engagement of new Sub-Processors. • Institutions have 1 month to object to engagement of the new Sub-Processors after being informed.	• TOPdesk must inform institutions 10 days prior to engagement of new Sub-Processors. • Institutions have 10 days to object to the new Sub-Processors after being informed.
Specification of Sub-Processors	Both Leaseweb and Microsoft (Azure) are listed as Sub-Processors engaged in the context of hosting.	-
Audits	Institutions may perform their own audits provided that: • It concerns a maximum of one audit per year, or more if there is a concrete suspicion that TOPdesk is not complying with the DPA and/or laws and regulations;	• Institutions may perform their own audits, provided that TOPdesk may impose reasonable requirements on these audits. These requirements are not further specified in the template DPA.

Element in DPA	SURF template DPA concluded between MBO Utrecht and TOPdesk	TOPdesk template DPA
	• The audit is announced at least 14 days in advance; and • The audit does not disrupt TOPdesk's normal business operations.	• TOPdesk will cover the costs of audits that require less effort, such as questionnaires and PEN-tests.
Personal Data breach notification	• TOPdesk must inform institutions within 24 hours after becoming aware of a Personal Data breach. • TOPdesk is obliged to: ○ have in place adequate policies and procedures to effectively handle data breaches; ○ maintain a record of Personal Data breaches within scope of the DPA ○ and to provide insight into these policies, procedures and records.	TOPdesk must inform institutions without undue delay.
Liability	• Institutions can be held liable for damages suffered by TOPdesk only insofar those damages were caused intentionally or by gross negligence • Compensation for damages suffered by TOPdesk in absence of intent or gross negligence by an institution is limited to €50.000, -	Any claim for damages against TOPdesk shall lapse 24 months after the claim arose.

The two templates are thus not identical. In certain respects, the SURF template is more advantageous for institutions than the TOPdesk template, and vice versa. For example, the Processing specifications in the TOPdesk template are more complete and thus provide more control. On the other hand, the provisions regarding the engagement of new Sub-Processors by TOPdesk in the SURF template are more favourable for institutions.

1.11 Test: Access Request

As part of this DPIA, a Data Subject Access Request was submitted to TOPdesk (see also Chapter 5 of the Technical Appendix). The request was drawn up by Privacy Company and submitted to TOPdesk by the institution where the technical research was carried out. In the request, TOPdesk was asked to provide information about the Processing of Personal Data from the four accounts that were created to carry out the technical investigation. The request clearly stated that the institution had already dealt with part of the request itself but needed further support from TOPdesk. The request contained an overview of the data of the four Users, including the unique IP addresses from which they connected and the address to which they connected. A copy of the Access Request is attached in Annex 3. Below, a timeline of the test is provided and some noteworthy observations.

Table 9: Timeline Access Request

Date	Event
06-08-2025	The institution sent the Access Request to TOPdesk
06-08-2025	TOPdesk sent a standard reply by TOPdesk referring to information sources and indicating that the Data Controller (i.e., the institution) must provide part of the information (also). The standard reply indicates that a response must be sent to have the request processed.
07-08-2025	The institution replied to TOPdesk's standard reply indicating that the questions were not fully answered. Reference was made to TOPdesk's obligation to comply with the request, in line with the DPA between the institution and TOPdesk.
19-08-2025	TOPdesk requested further clarification of the request in order to comply. One of the IP addresses that was initially provided in the request was incorrect.
19-08-2025	Correct IP address was shared.
19-08-2025	TOPdesk confirmed correction and continued with complying with the request.
11-09-2025[22]	TOPdesk provided the first substantive response to the Access Request. TOPdesk stated that they contacted Cloudflare and Microsoft for assistance in complying with the request. However, they had not provided the requested information yet. Therefore, TOPdesk invoked a 2-month extension based on Article 12(3) GDPR.
17-09-2025[23]	TOPdesk provided its full response, including information provided by Microsoft and Cloudflare. This information was incorporated into the first fully draft of this DPIA report (parts A-D).

---

[22] This response came within the statutory period of 1 month (Article 12(3) GDPR), despite having shared an incorrect IP-address in the original Access Request.

[23] This reply came within the 2-month extension period.

26-09-2025 – 10-10-2025[24]	E-mail communication between TOPdesk and Microsoft based on TOPdesk's review of the first draft of this DPIA report (parts A-D). TOPdesk reached out in relation to Privacy Company's conclusion that Microsoft acted as Independent Data Controller in responding to the DSAR. And requested them to comply (fully) with the DSAR. Eventually Microsoft and TOPdesk established that the infrastructure logs of Microsoft Azure do not contain personal data of the users of TOPdesk.

1.11.1 Reply by TOPdesk

TOPdesk – for their part – replied to the Access Request within the statutory period of 1 month required per Article 12(3) GDPR. The information provided by TOPdesk in its first response to the Access Request covered all data processing activities performed by TOPdesk and aligned with the observations made in this DPIA. The response was, however, not complete. TOPdesk was unable to fully comply with the request within the statutory period because they still needed information from Cloudflare and Microsoft. As a result, they had to extend the response period by two months, in line with Article 12(3) GDPR. In the first substantive reply TOPdesk was open about these circumstances and in their response indicated that they were in talks with Cloudflare and Microsoft to improve/accelerate this process in the future.

Another noteworthy observation during this test was that the first (automatic) reply from TOPdesk (06-08-2025) lists information sources where Data Subjects can read general information about the Processing of Personal Data through their use of TOPdesk. Further, the email refers Data Subjects to the Data Controller (i.e., the institution) for additional information. At the end of the email, the following is mentioned:

> *"If this didn't answer your question, please reply to this message to bring it to the attention of one of our privacy specialists."*

Although this email states that Data Subjects/institutions are required to take an additional step to actually file their request, TOPdesk will still process the requests even if the data subject does not follow up to the mail of TOPdesk. During the course of performing this DPIA, TOPdesk has removed the requirement to take an additional step from the text of their email as it was a redundant anti-spam measure.

TOPdesk's final response (17-09-2025) includes the reactions from Cloudflare and Microsoft.

1.11.2 Reply by Cloudflare

Cloudflare indicates that firewall logs (the DDOS protection) are stored for 31 days, meaning no relevant logs could be found for the period specified in the Access Request. The logs on website traffic are stored for 90 days by Cloudflare and were still available.

---

[24] The full e-mail conversation is confidential and can only be shared with TOPdesk approval...

A screenshot of the management page and an export of the totals per period have been added for the website traffic. In addition, an export of the first part of the raw logs on which these views are based has been added. These contain:

- The source IP-address of the request
- The hostname of the requested website
- The requested path
- The data and time of the request
- The 'UserAgent' string of the browser
- The status of cache for this request
- The response status of the server (when applicable)
- An internal reference for the cache

Though the file name suggests this raw data contains the first 1000 requests, it contained only 659 requests. These logs give a complete coverage, also of cached and denied requests.

TOPdesk indicated that the individual log lines were complex to export. This was due to a combination of the amount of data (almost 16,000 lines, while the system is designed to display a maximum of 10,000 lines) and the complex syntax of graphql, which is used to retrieve the data. Beside the sample of the first 659 loglines, TOPdesk also provided a count of the amount of loglines per timeframe of one hour and a screenshot of het management panel. Those two have a request count of 15,977. The stored traces from the testing contain 17.992 requests, so there is a discrepancy of 1.995 requests missing from the counts provided by TOPdesk. The cause of this discrepancy is unknown. Possibly the type of requests logged differ between the two systems. The inspection of the provided loglines did not show any relevant loglines missing.

1.11.3 Reply by Microsoft[25]

Initially, Microsoft responded they could not provide the log files. In response, TOPdesk entered into discussions with Microsoft about its responsibility to provide these log files. Microsoft eventually provided TOPdesk with a verbal explanation about the log files. This explanation revealed that Microsoft's infrastructure log files do not contain any personal data on TOPdesk end users.

Although Microsoft's confirmation email on this was not entirely clear, this explanation is plausible. The only log files to which TOPdesk does not have access are those at the infrastructure level, while the only personal data of TOPdesk end users that is processed unencrypted at that level are IP addresses. At the infrastructure level, these IP addresses are only logged if an exceptional situation occurs, such as an invalid data packet being received from that IP address. However, due to the network topology used by TOPdesk, invalid packets are filtered out earlier, at the firewalls. As a result, even in exceptional situations, no IP addresses of TOPdesk end users will be logged in the infrastructure logs.

In addition, Microsoft has provided TOPdesk with a way to determine which data is logged in the infrastructure.

---

[25] Microsoft's full reply is confidential and can only be shared with TOPdesk approval...

1.11.4 TOPdesk’s measures & commitments to prevent future delays

To prevent similar future delays in response time, TOPdesk has implemented some measures and made some commitments.[26]
In relation to Cloudflare:

- TOPdesk employees gained experience with graphql which enables them to respond to such Access Requests more quickly.
- TOPdesk updated its internal documentation to record the used code and references to additional documentation relevant to respond to such Access requests.
- TOPdesk updated its contact details of Cloudflare, making it easier to escalate urgent support requests, such as those relating to complying with an Access Request.

1.12 Exit plan

The Framework Agreement between SURF, institutions and TOPdesk stipulates that TOPdesk will draft a proposed exit plan within 3 months after entering into force of the Framework Agreement between an institution and TOPdesk. Institutions must consent to this proposal. The Data Processing Agreement shall remain in force until the exit plan has been fully executed.[27]

After execution of the exit plan, and consequential termination of the DPA, TOPdesk is obliged to delete/return all Personal Data to an institution. This must be done within a period specified in the exit plan or, in absence of a specified period, within one month after execution of the exit plan.[28] The assessed DPA templates both specify, in the annex, that after termination of the agreement, TOPdesk is obliged to delete any remaining (Personal Data in) back-ups within 90 days. Noteworthy in this regard is that TOPdesk retains back-ups of removed data after termination of an agreement for a minimum of 75, and maximum of 90, days, meaning TOPdesk technically enforces the retention periods specified in the assessed DPA’s.[29]

---

[26] TOPdesk’s final reply to the Data Subject Access Request, 17-09-2025, available at the request of SURF.

[27] SURF template DPA, Art. 12.1 in conjunction with art. 18 Framework Agreement.

[28] Art. 12.3 DPA

[29] The variation in retention time is caused by a manual verification step in the deletion process.

2. Personal Data

Which Personal Data TOPdesk processes is determined by and large by the specific use of the software by an institution. As discussed throughout Description of the system, the TOPdesk environment can be tailored to an institution's specific needs. For example, the way Cards are configured, and the information required to be provided in a Card, can be largely determined by institutions themselves. The chosen configuration, in part, determines which Personal Data is processed. In the table below, an overview of Personal Data likely to be processed as part of the scenarios assessed within this DPIA is presented. Institutions must assess for themselves whether they (intend to) process any additional Personal Data items in TOPdesk.

Table 10: Personal Data processed when using TOPdesk

Personal Data item	Description	Type
Asset ID	Unique number assigned to Asset	Normal
First and last name	Name of Operator/User	Normal
Gender	Gender of Operator/User	Normal
Contact details (e-mail address and (mobile) phone number)	Assigned to a User and visible in Calls submitted by the User	Normal
Department	Assigned to a User and visible in Calls submitted by the User	Normal
Location	Unique location assigned to an Asset such as a building, room in building, device (such as a laptop or desktop computer), "home", etc. The location is not directly related to a Data Subject and therefore cannot be used to track the location of a Data Subject	Normal
Role	Role within institution assigned to User/Operator (e.g. 'student', 'HR employee', 'teacher').	Normal
Student no./employee no.	Pseudo-identifier under which student/employee is known within the institution	Normal
Call code	Calls are registered under a unique number that can be traced back to the User that filed the Call	Normal
Visitor information	When configured, (Users and) Operators can register new/recurring visitors. The institution determines which Personal Data is registered of visitors. Potential Personal Data	Normal

	includes name, contact details, function, time of arrival and departure, reason of visit, number plate	
Device information	Through the Asset Management module, information about devices can be registered such as, but not limited to: type of device, IP address, MAC address, operating system, (hard/soft)ware version, location, assigned User, etc.	Normal
National identification number	The Dutch national law on education and vocational training (Wet educatie en beroepsonderwijs) requires that the national identification number of students must be processed as part of their registration with an educational institution (art. 8.0.3). If TOPdesk is used by institutions as part of the registration of (new) students, the national identification number may be processed in TOPdesk.	Sensitive
Unstructured Personal Data	Open text fields can be added to Cards and can contain Personal Data. Fields could be added to register, for example, budgets, nationality, number plate of vehicle, disabilities or functional limitations, etc. This is specifically relevant with regard to Authorisation Management.	Normal/sensitive/Special Category[30]
Search terms	In the SSP, analyses can be made of recently used search terms. These are not linked to a unique User, but the used search terms themselves may contain (sensitive or Special Category) Personal Data.	Normal/sensitive/Special Category

---

[30] Any type of Personal Data, including sensitive or Special Category Personal Data can be processed in open text fields.

Personal Data in log files: • Username • Unique User ID (32 characters) • IP address • Timestamps (date & time) • Other Personal Data, as configured by institutions themselves.	The use of TOPdesk by Operators and Callers generates Log files by default. Institutions can create custom rules for the creation of Log files. Examples are Log entries reflecting Actions performed on Cards or login attempts by Callers or Operators, including timestamps.	Normal/sensitive/Special Category[31]
Personal Data exchanged between TOPdesk and another program through Automated Actions based on API requests	Automated Actions, based on API requests, can be configured to exchange (personal) data between TOPdesk and another program (another TOPdesk environment or a different program/system).	Normal/sensitive/Special Category
Personal Data in standard TOPdesk cookies: • IP address • Session identifier (unique User ID) • URLs	By default, TOPdesk places a number of functional cookies. See §1.3.	Normal
Personal Data in optional Google Analytics cookie: • (Pseudonymised) IP-address • Characteristics of Device and Browser • Trail of visited pages	Institutions can choose to set a Google Analytics cookie in order to analyse the use of their TOPdesk environment. TOPdesk provides instructions on the most privacy friendly configuration of Google Analytics, but institutions remain free to configure the collection of Personal Data through the cookie. This may result in linking behaviour in TOPdesk to a Google account.	Normal/sensitive/Special Category[32]

As is apparent from the table above, institutions may process Special Category Personal Data as part of the envisioned use cases of TOPdesk. Noteworthy in this regard is that TOPdesk states, in its own template DPA, that its security measures provide

> *"adequate protection for the Processing of Personal Data, including <u>occasionally occurring</u> Special Categories of Personal Data. [TOPdesk] emphasises that the*

---

[31] As institutions can define custom log rules there is a possibility that sensitive and/or Special Category Personal Data is processed in log files.

[32] Page names could reveal sensitive/Special Category Personal Data.

> *software is not designed or intended for the large-scale Processing of Special Categories of Personal Data […]”.*[33]

---

[33] TOPdesk template Data Processing agreement v.2025, Appendix, p. 9.

3. Data Processing

In this section of Part A, an overview is provided of Personal Data Processing Activities that result from the use cases.

In terms of Processing Activities, a distinction is made between primary and optional Processing Activities. Primary Processing Activities refer to Processing Activities necessary for the use cases that fall within the scope of this DPIA.

Table 11: Primary Processing Activities

Primary Processing Activities		
Sign in with credentials	Create a Call	Submit a Call
Access Personal Data in a Call	Edit Personal Data in a Call	Forward/Share Personal Data from a Call (internal or external)
(de)Escalate a Call	Upload attachment containing Personal Data (in meta- or content data)	Sending of emails related to Calls
Close a Call	Storage of User Personal Data (in Calls)	Anonymise Personal Data
Delete Personal Data	Archive Personal Data	Create backups of Personal Data
Sign out	Create User/Operator	Edit Personal Data of User/Operator
Delete User/Operator	Registration of information about individual usage of TOPdesk (creating log files)	Analysis/monitoring of Personal Data in log files
Network traffic analyses (Cloudflare)	Encryption/decryption	Access to Personal Data by TOPdesk in context of (helpdesk)support
Access to Personal Data by TOPdesk in context of consultancy services		

Optional Processing Activities refer to Processing Activities which are not necessary for the use cases assessed in this DPIA but may be performed due to the specific (desired) use of TOPdesk by an institution, such as use of Google Analytics or the collection of (User) feedback.

Table 12: Optional Processing Activities

Optional Processing Activities		
Create Knowledge Item from Call	Usage analysis (Google Analytics)	Collection and Processing of chats (optional use of Hello Ebbot AB's Live chat and/or AI Chatbot functionalities)

Collection of feedback (optional use of Insocial)	Testing TOPdesk (when done with production data)	

4. Purposes of the Processing

This section of Part A describes the purposes institutions may have when using TOPdesk. These purposes are based on the use cases assessed within this DPIA and the purposes described in the Annex of the SURF template DPA.

In the Higher Education Reference Architecture (HORA), service management systems (SMS) and IT management systems (IMS) such as TOPdesk are positioned within the domain of "business operations". An SMS plays a central role in internal service provision to students and employees of institutions by managing, designing, building, delivering, operating and controlling services offered to students and employees.[34] An IMS is a system used in the context of information security and IT system management.[35]

The purposes of the Processing Activities performed as part of the implementation of TOPdesk as SMS and IMS are described in general in the SURF template DPA as follows:

1. Performance of the Framework Agreement
2. Hosting of the software environment
3. Providing support to institutions by TOPdesk (if and insofar as instructed to do so by an institution)
4. Providing consultancy to institutions by TOPdesk (if and insofar as instructed to do so by an institution)
5. Monitoring of the technical application and operational management (SaaSOps)

The TOPdesk template DPA does not specify any purposes of Processing Activities. Instead, it leaves room for institutions to specify the purpose(s) of the Processing Activities.

The GDPR requires that the Processing purposes for each Processing Activity be specifically identified. The specific purposes of the Processing Activities performed by individual institutions are not in scope of this DPIA, as such an assessment would not concern the use of TOPdesk as SMS and IMS. However, the purposes for which the institutions use TOPdesk in relation to Processing Activities that fall within the scope of this DPIA must all be directly related to the 5 general purposes described above.

Each institution has/must set up its own Record of Processing Activities (hereinafter: 'ROPA') in which these specific purposes are identified. Institutions, as controllers, must independently inform Data Subjects about their (purposes of) Processing Activities via its information material, such as the privacy statement on their website.

Institutions may have related purposes, such as recording additional information about the use of TOPdesk through the creation of custom log rules for security purposes.

---

[34] SURF, Hoger Onderwijs Referentie Architectuur (HORA), Servicemanagementsyteem, https://hora.surf.nl/index.php/Id-c076576d-c8ca-8c5f-c5ee-9bcea53ff5a0 <accessed 06-08-2025>.

[35] SURF, Hoger Onderwijs Referentie Architectuur (HORA), IT-management systeem, https://hora.surf.nl/index.php/Id-da56a123-84fe-6e6f-1182-94521c0126d6 <accessed 06-08-2025>.

5. Involved Parties

Table 13: Overview of parties involved in Personal Data Processing

Party	Role	Description of involvement
Students, employees of institutions and external parties, visitors	Data Subject	Data Subjects will use TOPdesk. Their Personal Data is processed as part of their use or when entered by another User.
SURF members	Data Controllers	Institutions offer TOPdesk to Data Subjects and determine the means and purposes of Processing.
TOPdesk	Data Controller	As a service provider, TOPdesk acts as Data Controller for the following purposes:[36] • Customer relationship management • Customer support • Marketing • Improve services • IT & network security • Prevention/detection of fraud • Comply with legal obligations
	Data Processor	As supplier, TOPdesk acts as a Data Processor for the following purposes[37]: • Performance of the Framework Agreement • Hosting of the software environment • Providing support to institutions by TOPdesk (if and insofar as instructed to do so by an institution) • Providing consultancy to institutions by TOPdesk (if and insofar as instructed to do so by an institution) • Monitoring of the technical application and operational management (SaaSOps)
TOPdesk Sub-Processors		
TOPdesk Belgium	Sub-Processor of TOPdesk	• Support • Technical administration/management
TOPdesk Denmark	Sub-Processor of TOPdesk	• Support • Technical administration/management
TOPdesk Germany	Sub-Processor of TOPdesk	Technical administration/management
FOX-IT	Sub-Processor of TOPdesk	Security Information and Event Management (SIEM) system, monitoring server logs and configuration files on the TOPdesk SaaS network to detect known attack patterns and threats.

---

[36] TOPdesk Privacy Statement, 04-01-2025, https://www.topdesk.com/en/privacy-policy/.

[37] SURF template DPA, Annex A.

Cloudflare U.S.	Sub-Processor of TOPdesk	Manages SSL certificates for encrypting connections and adds additional security like DDOS protection. The Cloudflare Content Delivery Network is used to route traffic to TOPdesk SaaS environments.
Hosting provider: Microsoft Ireland Operations ltd. (for Azure)	Sub-Processor of TOPdesk	Manage the hardware used to run all servers for TOPdesk SaaS services.
Data centre provider: Microsoft Ireland Operations ltd. (for Azure)	Sub-Processor of TOPdesk	Manage the hardware used to run all servers for TOPdesk SaaS services.
	Independent Data Controller	As found during the Test: Access Request, Microsoft determined itself that it will not comply with the Access Request. In making this decision, Microsoft acts as Independent Data Controller.
84 Codes AB (CloudAMQP)	Sub-Processor of TOPdesk	The message bus enables the services within the TOPdesk application to communicate information (data) to each other. This information can also contain Personal Data, for example audit trail information. This solution is active in all Azure Hosting locations. Processing takes place within the EEA. TOPdesk entered into a Processing agreement with 84 Codes AB in 2022, as required by the GDPR.
Optional third parties		
Unspecified third parties such as, but not limited to, Google (for YouTube integrations or use of Google Analytics), Blackboard and any other third party with which an institution selects to exchange Personal Data.	(Independent/joint) Data Controller or (Sub-)Processors of institution	Institutions can choose to exchange Personal Data with third parties by various means, for example: • Exchange can take place with third party software through Automated Actions based on API requests. • Calls can be (partially) forwarded to a third party in order to be resolved, in cases where Operators are not able to resolve the Call. • Institutions can choose to enable Google Analytics, in which case Personal Data is shared with Google. • Institutions can create web integrations, in which case Personal Data can be shared with third parties (e.g. Google in case a YouTube-integration is created)

		These third parties may qualify as Data Controller or (Sub-)Processors of an institution. Institutions must determine this on a case-by-case basis. The SURF template DPA does not list any such third parties.
Hello Ebbot AB	Sub-Processor of TOPdesk	Allows TOPdesk to integrate and support Ebbot Live Chat and Ebbot AI Chatbot. Optional feature, not included in the instructions provided to TOPdesk in the SURF template DPA
Insocial	Sub-Processor of TOPdesk	Allows TOPdesk to support and integrate with Insocial feedback solutions. Optional feature, not included in the instructions provided to TOPdesk in the SURF template DPA

Changes in TOPdesk's Sub-Processors are announced through TOPdesk's SaaS maintenance page.[38] Institutions must subscribe for active updates about changes to Sub-Processors through this page.

---

[38] TOPdesk, SaaS maintenance page, https://status.topdesk.com/ <last accessed 04/09/2025>.

6. Interests in the Data Processing

6.1 Main Data Subjects: Students and employees of institutions

Students and employees of institutions have an interest in a well-functioning and reliable service management system, in which the institution handles their Personal Data with care. In addition, those involved have an interest in the discreet handling of information relating to accidents/inappropriate behaviour in the context of social safety, HR-related information and sensitive information about devices, incident/application and complaint management, and other sensitive information available to the institution, whereby the institution takes technical and organisational measures to prevent unauthorised use/access. Finally, students and employees have an interest in ensuring that their Personal Data is not processed unnecessarily or unlawfully in TOPdesk.

6.2 Other Data Subjects: employees of third parties and visitors of institutions

Employees of third parties and visitors of institutions whose Personal Data is processed by an institution in TOPdesk have an interest in ensuring that their Personal Data is not processed unnecessarily or unlawfully in TOPdesk also.

6.3 Controller(s): institution(s)

A service management system is an important part of the operational management and administrative processes of an educational institution. The importance of institutions using a service management system lies in the efficient handling of questions, requests and incidents and compliance with the requirements of the various relevant laws. Freedom of choice in the systems they use and control over the Personal Data in those systems are important in this regard, as are continuity of operations and employee- and student satisfaction. In addition, it is in the interests of institutions to handle the Personal Data of employees and students carefully and lawfully, among other things to avoid enforcement. Finally, the institutions have a major interest in maintaining their reputation as reliable providers of higher education.

6.4 Processor: TOPdesk Netherlands

The Dutch education sector is an important market for TOPdesk Netherlands. TOPdesk has a (business) interest in providing a high-quality service and maintaining its market position, while complying with the requirements of relevant legislation and regulations. For example, TOPdesk has an interest in adequately securing the system and the Personal Data it contains, applying data minimisation and supporting institutions in the correct use of TOPdesk. Quality, information security and privacy are central to this.

Additionally, as TOPdesk Belgium, TOPdesk Denmark and TOPdesk Germany (all Sub-Processors of TOPdesk) fall under the same parent company, they have the same interests as described for TOPdesk Netherlands above.

6.5 Sub-Processors

The Sub-Processors Fox-IT, Cloudflare, Microsoft and 84 Codes AB (CloudAMQP) have a commercial interest in providing the services that enable TOPdesk to deliver their system as a SaaS solution. They also have an interest in complying with laws and regulations.

6.6 Optional parties: (Independent/joint) Data Controller or (Sub-)Processors of institution

Insofar as institutions choose to use the optional features/services provided/facilitated by third parties, such as Google, Blackboard, Hello Ebbot AB and Insocial (see Table 13: Overview of parties involved in Personal Data Processing), they too have a commercial interest in providing the services that enable TOPdesk to deliver their system as a SaaS solution. Further, they also have an interest in complying with relevant laws and regulations.

7. Locations of the Data Processing

7.1 TOPdesk

The SURF template DPA, in article 8, allows for the transfer of Personal Data outside of the EEA with consent of an institution. However, Annex A of the completed DPA between the tested institution and TOPdesk does not specify, and thus does not provide consent for, any transfers of Personal Data.[39] Similarly, the TOPdesk template DPA, in article 11, allows for the ex-EEA transfer of Personal Data with consent of an institution. However, no Annexes are attached to the template DPA in order to facilitate the providing of consent for ex-EEA transfers by an institution.[40] This indicates that use of the TOPdesk SaaS services does not require the transfer of Personal Data. Nonetheless, during the technical research that was performed in the context of this DPIA, a transfer of the IP address of Data Subjects accessing a TOPdesk environment was identified. This Personal Data was exported by TOPdesk and imported by Cloudflare in the context of the DDoS protection performed by Cloudflare as Sub-Processor.

Apart from the transfer identified in the technical research, no other transfers of Personal Data to a third country or to an international organisation outside the European Economic Area ('EEA') were identified during this research. TOPdesk facilitates the storage of Personal Data within the European Economic Area ('EEA'). Institutions are free to choose which data region they select. Options include the Netherlands, Germany, Ireland, and more. Back-ups of Personal Data made by TOPdesk are located in the same region as that which is selected by the institution (e.g. West-Europe), but at a different location (e.g. Germany instead of the Netherlands). In principle, the Personal Data remains within the selected region. However, with explicit written consent by an institution Personal Data may be transferred outside the EEA. Such a transfer may occur, for example, in case of a support request by an institution which is handled by a TOPdesk employee located outside the EEA – but only if remote access setting has not been set to EU, see §1.8. In the context of this DPIA it is assumed that institutions a) make use of the opt-out for ex-EEA access for support purposes and b) do not make use of the opt-in to allow TOPdesk support personnel to log in to their TOPdesk environment, meaning no transfer of Personal Data takes place in the context of support by TOPdesk personnel.

Regarding Personal Data transfers arising from complying with court or gag orders to share customer Personal Data with foreign entities such as intelligence services, TOPdesk has confirmed that it has not received any such orders. As TOPdesk is a Dutch owned company, foreign legislation on the basis of which TOPdesk may be obliged to share data with foreign authorities (e.g., US CLOUD Act) does not apply.

7.2 TOPdesk Sub-Processors

In principle – based on both the SURF template DPA and TOPdesk template DPA – all of TOPdesk's Sub-Processors as listed in Involved Parties Process Personal Data within the EEA. With the exception of Cloudflare, these Sub-Processors are all established in countries within the EEA; Cloudflare is established in the United States of America.

---

[39] Article 8 and Annex A ('Doorgiften buiten de Europese Economische Ruimte'), SURF Model Data Processing agreement, version 3.0, April 2019.

[40] Article 11 and 'Appendix – Specification of personal Data Processing', TOPdesk Model Data Processing agreement, v.2025.

Like stated above, the SURF template DPA does not exclude ex-EEA Personal Data transfers. However, the completed DPA between MBO Utrecht and TOPdesk shows that no necessary transfers of Personal Data take place via TOPdesk's Sub-Processors either.

The Sub-Processor 84 Codes AB processes exclusively within the EEA. This was confirmed during the technical research and by TOPdesk in their reply to the Data Subject Access Request.[41]

7.2.1 Microsoft (Azure)

The Data Processing Agreement between TOPdesk and Microsoft (Azure) does, however, allow for the transfer of Personal Data outside the EEA; onward transfers are not excluded in the DPA either[42] Moreover, as Microsoft is a US based Sub-Processor, they fall within scope of US law (e.g. CLOUD Act) and could therefore be forced to transfer Personal Data outside the EEA, to the US; regardless of whether an institution has provided consent. TOPdesk has implemented several measures to minimise this risk, most notably:

- Encrypted storage in Microsoft Azure. Decryption keys for the storage locations are stored in a hardware security module, the key vault. When an application, like the database, needs a secret key, it retrieves it from the Vault and keeps it in memory for use during a predefined period of time. Access to the Vault is managed by an identity server of Azure.
- Yearly review of audits by TOPdesk on Microsoft's statements in relation to ex-EEA data transfers.
- Use of a separate domain with internal test environments to troubleshoot hosting issues to ensure that tests or troubleshooting steps never accidentally reveal customer data to a third party.
- Application of pseudonymisation – where possible – in its product and hosting services. For instance, data storage locations only contain the unique environment ID of an institution's TOPdesk environment (instead of the institution's name), and requester names are separated from their requests within the database. This reduces the options for Microsoft to comply with legal data Access Requests under the Cloud Act since they cannot identify which data belongs to which person or institution.
- A clause in the Data Processing Agreement requiring Microsoft to attempt to inform institutions about, and forward, third party orders to disclose Personal Data, challenge any such orders and indemnify Data Subjects in case Personal Data has been transferred – in so far legally permitted. The DPA, however, does not contain a hard obligation for Microsoft to inform Data Controllers of an inability to comply with this clause if they receive a third-party order accompanied by a gag order (also known as a 'canary clause'[43]).

Even though a Data Transfer Impact Assessment (DTIA) is not currently required for Controllers or Processors that are certified under the Data Privacy Framework, as Microsoft US is[44], TOPdesk has performed a transfer risk assessment taking into account the

---

[41] TOPdesk's reply to the Data Subject Access Request, 05-09-2025, available at the request of SURF.

[42] Microsoft Products and Services Data Protection Addendum Apr. 2025, Section 'Data Transfers and Location', p. 16-17.

[43] Here, a canary clause refers to a clause in the DPA between TOPdesk and, for example, Microsoft or Cloudflare, which states that Microsoft/Cloudflare must inform TOPdesk of their inability to comply with (a specific clause in) the DPA. Such a clause would not require the (Sub-)Processor to inform TOPdesk of the specific reason(s) for their inability to comply with this clause – which could be because they have received a gag order – but only of that fact that they cannot comply.

[44] 'Data Privacy Framework Program', < https://www.dataprivacyframework.gov/list> last accessed 01/10/2025.

measures mentioned above. TOPdesk concluded that the risk of transfer is very low. This risk, however, cannot be fully mitigated given the conditions agreed upon in the Data Processing Agreement between TOPdesk and Microsoft. Moreover, TOPdesk has indicated that transfers cannot be technically excluded.[45] If a transfer were to take place, this would constitute a violation of the DPA between TOPdesk and an institution – under the condition that the SURF template DPA is utilised. If institutions opt to make use of the TOPdesk template DPA, transfers are only prohibited, and a transfer would thus only constitute a violation of the DPA, under the condition that there are no transfers specified in the Appendix of the DPA.

7.2.2 Cloudflare

The Data Processing Agreement between TOPdesk and Cloudflare allows for the transfer of Personal Data outside the EEA.[46] Specifically, the DPA mentions the transfer of:

- Personal Data in log files, such as IP addresses, end usernames and email addresses
- Personal Data in content data

As stated, the technical research confirmed that there is a transfer of Personal Data to Cloudflare, but this concerned only the IP addresses of Data Subjects accessing a TOPdesk environment in the context of DDoS protection. TOPdesk indicated that this transfer cannot be technically excluded.[47] Cloudflare is certified under the Data Privacy Framework, meaning that the adequacy decision issued by the European Commission for the United States of America applies to them.[48] However, the transfer is not reflected in any of the DPAs in scope of this DPIA., while the DPA does contain the EU Standard Contractual Clauses as additional transfer mechanism.

US law

As Cloudflare is a US based Sub-Processor which falls within scope of US law, TOPdesk has implemented several measures to minimise the risk associated with transfers, most notably:

- Encryption (HTTPS and HSTS preloading) of traffic between the TOPdesk SaaS environment and the Content Delivery Network provided by Cloudflare. This prevents access to, and (effective) transfer of, content data while in transit between TOPdesk and Cloudflare.
- A clause in the Data Processing Agreement requiring Cloudflare to inform institutions, where legally allowed, of third-party orders to disclose Personal Data, challenge any such orders and indemnify Data Subjects in case Personal Data has been transferred.
- Cloudflare publishes periodic Transparency Reports which contain canary clauses, TOPdesk monitors these Transparency Reports. To date, the canary clause has not been removed meaning there is no reason to assume that Cloudflare has complied with government access requests for Personal Data of TOPdesk end users.
- Yearly review of audits by TOPdesk on Cloudflare's statements in relation to ex-EEA data transfers.

---

[45] TOPdesk's reply to the Data Subject Access Request, 05-09-2025, available at the request of SURF.

[46] Cloudflare Data Processing Addendum, Art. 6.

[47] TOPdesk's reply to the Data Subject Access Request, 05-09-2025, available at the request of SURF.

[48] 'Data Privacy Framework Program', < https://www.dataprivacyframework.gov/list> last accessed 10/09/2025.

Despite the above measures, access to, and transfer of, content data is in principle still possible as the traffic is decrypted in the regional hosting location and inspected for known patterns by Cloudflare. As such, for a short period, Cloudflare has access to the decrypted Personal Data in content data and could be legally required to transfer such data to a US authority based on US law (e.g. CLOUD act). Additionally, the IP address of the end user accessing the TOPdesk environment is (temporarily) stored in one central location in the US for traffic analysis, meaning this Personal Data is also subjected to US law.

The tests that were performed in the context of this DPIA did not provide definitive conclusions regarding the locations of the Processing Activities performed by Cloudflare. However, based on the architecture, the following locations of Processing Activities could be established:

- Cloudflare data centre closest to the datacentre chosen by the institution, where the full content of the HTTP requests is processed.
- Cloudflare data centre close to the User of TOPdesk, where IP addresses are processed.
- Cloudflare operations centre in the US, where IP addresses are processed.

In conclusion, transfer of Personal Data outside the EEA takes place through TOPdesk’s Sub-Processor Cloudflare; namely, the IP-addresses of Users accessing their TOPdesk environment, which are processed in the US. Such transfer constitutes a violation of the DPA between TOPdesk and an institution – under the condition that the SURF template DPA is utilised. Further, there is a chance that transfers take place based on US Law, as both Cloudflare and Microsoft are subject to those laws and may be required to grant US authorities access to Personal Data of TOPdesk end users. Due to the measures implemented by Microsoft, Cloudflare and TOPdesk respectively, there is however no indication that transfers of such a nature have occurred.

7.3 Institutions

As stated, institutions can select the region and location themselves. As all institutions are located within the Netherlands, it is assumed that their Processing location(s) will also be within the EEA.

8. Techniques and methods of data Processing

The use of TOPdesk as assessed within this DPIA does not involve any form of automated decision-making, profiling or big data Processing by TOPdesk. Cloudflare has an automated process to decide if a user will get an extra challenge presented by Cloudflare or not. This automated process had no legal effects, nor does it significantly impact the Data Subject, so it does not qualify as automated decision making within the meaning of article 22 GDPR.

9. Legislative and Policy Framework

In addition to the GDPR, the following Dutch national legislation and regulations may apply to the use of TOPdesk by educational institutions:

Table 14: Additional laws and regulations

Legislation/regulation	Relevant article(s) (optional)
Wet op het hoger onderwijs en wetenschappelijk onderzoek	7.31e., 7.52., 7.39
Wet educatie en beroepsonderwijs	2.3.6.a, 8.0.3, 8.1.1., 8.1.1.a, 8.5.a.7
Wet algemene bepalingen burgerservicenummer	10, 11, 12, 13
Baseline Informatiebeveiliging Hoger Onderwijs	N/A
Telecommunicatiewet (national implementation of ePrivacy Directive)	11.7a

9.1 Wet op het hoger onderwijs en wetenschappelijk onderzoek (Higher Education and Scientific Research Act)

The Higher Education and Scientific Research Act forms the legal framework for universities and universities of applied sciences in the provision of education. The Act provides a legal basis for the Processing of certain Personal Data of students. In case a university or university of applied sciences uses TOPdesk in the context of the registration of (new) students, the Act, in conjunction with the Wet algemene bepalingen burgerservicenummer (General Provisions Act on the Citizen Service Number), provides the legal basis for the Processing of national identification numbers.

9.2 Wet educatie en beroepsonderwijs (Vocational Education and Training Act)

The Vocational Education and Training Act forms the legal framework for vocational education institutions. The Act provides a legal basis for the Processing of certain Personal Data of students. In case a vocational education institution uses TOPdesk in the context of the registration of (new) students, the Act, in conjunction with the Wet algemene bepalingen burgerservicenummer (General Provisions Act on the Citizen Service Number), provides the legal basis for the Processing of national identification numbers.

9.3 Wet algemene bepalingen burgerservicenummer (General Provisions Act on the Citizen Service Number)

Government bodies may use the citizen service number when Processing Personal Data in the context of performing their duties (Article 10 of the General Provisions Act on the Citizen Service Number). Educational institutions are not, in principle, considered government bodies, except when they have been assigned public authority tasks.

9.4 Baseline Informatiebeveiliging Hoger Onderwijs (Baseline Information Security Higher Education)

SURFibo has developed a model information security policy for higher education. The policy addresses the relevant information security measures in accordance with ISO 27002 that must be taken in higher education.

9.5 Telecommunicatiewet (Telecommunications Act, national implementation of ePrivacy Directive)

The Telecommunications Act governs, among other things, the Processing of Personal Data through cookies. Institutions can enable Google Analytics in TOPdesk. Depending on the way the institution configures Google Analytics, the Telecommunications Act may apply. Further, institutions may create web integrations in TOPdesk which may result in the placing of cookies on a User’s device/browser. Depending on the types of cookies, the Telecommunications Act may apply.

10. Data Retention Periods

A Data Controller may retain Personal Data for as long as it is necessary for the purpose for which it was collected, according to the GDPR (Article 5 GDPR). After that, the Controller must destroy the data, unless the Controller is obliged to retain it, for example because this is required by law.

The following paragraphs describe relevant information on retention periods in the appendix to SURF's template DPA, TOPdesk's template DPA, the retention periods in TOPdesk and the retention periods applied by Microsoft.

10.1 Retention periods in legal documentation

10.1.1 SURF template DPA

The SURF template DPA, and the DPA between MBO Utrecht, the institution where the technical research was performed, and TOPdesk, contain the following provisions on retention periods in Annex A:

> *"- After termination of the Agreement and/or after termination of the Services, the Processor [TOPdesk] is obliged, upon written request from an authorised representative of the Controller [institution], to return the Personal Data to the Controller [institution] within 30 days (or to offer the Controller [institution] the possibility to retrieve the Personal Data digitally). Any remaining (copies of) Personal Data and/or back-ups shall be destroyed by the Processor [TOPdesk] within 90 days of termination.*
>
> *- During the term of the Agreement, the Controller [institution] may store or delete data in the software at its own discretion. In addition, the Controller [institution] may make its own back-ups of the data in the software environment. The Processor [TOPdesk] has no insight into or influence on the manner in which the Controller [institution] uses these options. The Processor [TOPdesk] will store back-ups of the data in the Processor's [institution's] environment for a period of 30 days. After this period, but no later than 90 days, the back-ups will be deleted."*

10.1.2 TOPdesk template DPA

The TOPdesk template DPA contains the following provisions on retention periods in the Annex:

> *"Duration of the Processing*
> *After termination of the Agreement and/or after termination of the Services by the Controller, the Processor is obliged, upon written request from an authorised representative of the Controller, to return the Personal Data to the Controller within thirty (30) days or provide the Controller with the opportunity to retrieve the data digitally. Any remaining (copies of) Personal Data and/or back-ups must be destroyed by the Processor within ninety (90) days after termination.*
>
> *Retention Periods*

> *All actions related to the retention, preservation, and deletion etc. of Personal Data, both during and after the completion of the Agreement, fall solely under the responsibility of the Controller. These actions are related to the setup of data management. TOPdesk provides standard software that supports the automation of these processes. It is the responsibility of the Controller to use this software correctly. This also applies to the management of external back-ups and similar procedures."*

10.2 Retention periods TOPdesk

TOPdesk contains multiple features (see also §1.2.13) that enable an institution to implement, and apply, its retention policy to the Personal Data processed in TOPdesk. Specific retention periods are determined by institutions themselves as Data Controllers and must be aligned with the GDPR requirement that Personal Data is not stored for longer than necessary for its Processing purpose(s), unless legal or statutory requirements require otherwise.

After an institution deletes Personal Data in TOPdesk, the data will remain available for a short period in a back-up.

Retention periods of back-ups are as follows:

Table 15: Retention periods of TOPdesk back-ups

Back-up	Retention period
Continuous database back-up	35 days
Daily off-site attachment back-up	24 hours
Local back-up (by institution itself)	Determined by institution
Back-up of deleted environment	75 days

Furthermore, TOPdesk has implemented a retention policy in relation to the Personal Data it processes in log files:

Table 16: Retention periods of TOPdesk log files

Type of log file	Retention period
Application access logs (containing all login attempts and information to identify the source, such as IP address)	6 months
Full access logs (containing all activity in an institution's TOPdesk environment, including settings changes, permissions changes, and new accounts)	3 days
Application logs (containing all actions and troubleshooting information regarding a TOPdesk environment)	10 days
Service logs (containing all actions and troubleshooting information regarding services used by all TOPdesk environments in one hosting location)	90 days

SaaS hosting server logs (containing all log-in attempts and relevant actions for the SaaS hosting server)	30 days
Security logs in the FOX-IT SOC (containing all log-in attempts and relevant actions for the SaaS hosting server)	90 days

10.3 Retention periods Microsoft

As TOPdesk is hosted on Microsoft Azure, retention periods at Microsoft are also relevant in light of this DPIA.

The DPA between TOPdesk and Microsoft states the following on retention periods:

> *“Microsoft will retain Customer Data that remains stored in Online Services in a limited function account for 90 days after expiration or termination of Customer’s subscription so that Customer may extract the data. After the 90-day retention period ends, Microsoft will disable Customer’s account and delete the Customer Data and Personal Data stored in Online Services within an additional 90 days, unless authorized under this DPA to retain such data.”*[49]

---

[49] Microsoft, Products and Services DPA (April 1, 2025), p. 18.

Part. B Lawfulness of the Processing

The second part of the DPIA assesses the lawfulness of the data Processing. This part contains an assessment of the legal grounds of both the educational institutions and Adobe, the Processing of special Personal Data, the application of purpose limitation, the necessity of the Processing, and the application of Data Subjects' rights.

11. Legal grounds

To be permissible under the GDPR, the Processing of Personal Data must be based on one of the legal grounds mentioned in Article 6 (1) GDPR.

Before addressing the applicable legal bases for the Processing, it is first necessary to outline the context in which the Processing occurs. This includes not only defining the roles of the parties involved but also examining the contractual framework that governs their relationship. TOPdesk is a Data Processor when it comes to providing the contracted Service Management Software. Furthermore, TOPdesk also Processes Personal Data for its own purposes collected as Data Controller.

11.1 Contractual context and role determination

Based on both the SURF template DPA and the DPA concluded between TOPdesk and the institution where the technical research was performed, TOPdesk acts as Data Processor, and institutions act as independent Data Controllers, for the following purposes:

1. Performance of the Framework Agreement
2. Hosting of the software environment
3. Providing support to institutions by TOPdesk (if and insofar as instructed to do so by an institution)
4. Providing consultancy to institutions by TOPdesk (if and insofar as instructed to do so by an institution)
5. Monitoring of the technical application and operational management (SaaSOps)

The TOPdesk template DPA leaves room for institutions to specify the purposes for which TOPdesk Processes Personal Data as Processor for institutions, i.e. the Data Controller.

Additionally, based on TOPdesk's privacy statement published on its website[50], TOPdesk acts as Data Controller for the following purposes:

- Customer relationship management
- Customer support
- Marketing
- Improve services
- IT & network security
- Prevention/detection of fraud
- Comply with legal obligations

The Personal Data Processing for these purposes are collected by TOPdesk as Data Controller, not as Processor, and therefore do not qualify as further Processing Activities as defined in Article 6(4) GDPR.

11.2 Legal grounds for institutions

This section assesses the potential legal bases for educational institutions for using TOPdesk.

As this is an umbrella DPIA, the actual legal grounds relied upon by institutions when Processing Personal Data as Data Controller for the purposes mentioned above cannot be

---

[50] 'TOPdesk Privacy Statement', < https://www.topdesk.com/en/privacy-policy/> last accessed 10/09/2025.

identified in this DPIA. It is up to the institutions themselves to identify these legal grounds and assess to what extent they apply. However, based on the specified purposes and envisioned use cases assessed in this DPIA, it is likely that they will mainly rely on the legal basis of legitimate interest (Article 6(1)(f) GDPR) for the Processing of Personal Data with TOPdesk. In order to determine whether an institution has a legitimate interest when doing so, they must first perform legitimate interest assessments.[51]

11.3 Legal grounds for TOPdesk

When acting as a Processor, TOPdesk is instructed by an institution and works on behalf of that organisation. The legal grounds for Processing used by the institution then also apply to TOPdesk as a Processor.

When acting as a Data Controller, TOPdesk determines its own legal grounds for the Processing of Personal Data. These legal grounds are specified in TOPdesk's privacy statement:

Table 17: Processing purposes of TOPdesk as Data Controller

Purpose	Legal ground	Personal Data
Customer relationship management	Legitimate interest	• Contact details • Payment details • Website usage data (optional)
Customer support	Legitimate interest	• Contact details • Message contents • Website usage data (optional)
Marketing	Consent & Legitimate interest	• Contact details • Message contents • Website usage data
Improve services	Consent & Legitimate interest	• Contact details • Message contents • Other data (optional)
IT & network security	Compliance with a legal obligation & Legitimate interest	• Contact details • Message contents • Website usage data
Prevention/detection of fraud	Compliance with a legal obligation & Legitimate interest	• Contact details • Message contents • Website usage data
Comply with legal obligations	Compliance with a legal obligation & Legitimate interest	• Contact details • Message contents • Website usage data • Customer Agreement content

---

[51] Article 6(1)(f) GDPR and Recital 47 GDPR.

The Personal Data items mentioned in the Table above are defined by TOPdesk as follows (underlining added by Privacy Company):

- *"Contact details refer to all Personal Data that can be used to identify and contact you. This includes your name, function title, gender, email address, telephone number, social media pages, the name of the company you work for, and contact details for your company.*
- *The message contents, for instance the body of an e-mail that you sent us or the information you submit in a form on our website, may also include information that can be used to identify you.*
- *Website usage data is all information gathered while you use websites and/or services. The website you came from, search teams used, your IP address, browser signature, which pages you open, etc. This often doesn't directly identify you personally, but it might.*
- *Other data may be collected during user (experience) research to help us understand how users experience our products and services. When you participate in research where other data is used in addition to your contact details, we'll explain how this data is used and ask for your consent to use this information before starting to collect it."*[52]

TOPdesk has stated in communication between Privacy Company and itself that it does not process any Personal Data it has collected as Processor for its own purposes.[53] During the technical research, no evidence was found which implied Processing of customer data by TOPdesk for its own purposes. This, however, is not fully clear from the text of TOPdesk's privacy statement. The privacy statement is divided into a section on Processing Activities performed by TOPdesk as Processor and a section on the Processing Activities performed by TOPdesk as Controller. From the text, it is not fully clear that the Personal Data collected as Processor is never used by TOPdesk as Controller, which may create uncertainty for institutions and their Data Subjects. Furthermore, the definitions of certain Personal Data items do not clarify that this does not concern Personal Data collected by TOPdesk as Processor and subsequently processed as Data Controller (see the underlined text in TOPdesk's privacy statement above and below):

- *Message contents* is not defined exhaustively, and it is therefore not clear whether this may concern Personal Data collected from messages which TOPdesk has received as Data Processor.
- *Website usage data* is defined in such a way that it includes information of Data Subjects gathered during their use of TOPdesk's services, which may imply that this also concerns Personal Data collected by TOPdesk as Processor from Data Subjects using TOPdesk.

As these Personal Data items are mentioned under the section covering TOPdesk as Data Controller, it can be assumed that data from educational environments (where TOPdesk is data processor) is not used. However, no explicit guarantees are provided in the statement which creates some uncertainty.

Lastly, TOPdesk mentions multiple legal grounds for most of its own Processing purposes (e.g. both Compliance with a legal obligation & Legitimate interest for the prevention/detection of fraud). This does not provide sufficient transparency in order to determine whether that Processing is legitimate as meant in Article 5(1)(a) jo. Article 6(1) GDPR.

---

[52] 'TOPdesk Privacy Statement', < https://www.topdesk.com/en/privacy-policy/> last accessed 10/09/2025 [underline added].

[53] TOPdesk's full reply is available at the request of SURF.

12. Special Category Data

Special Category of Personal Data are *"Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the Processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation"* (Article 9 (1) GDPR).

With Special Categories of Personal Data, the principle is one of prohibition: these data may not be processed. The law contains specific exceptions to this rule (which must be interpreted strictly)[54], for instance when the Data Subject has explicitly consented to the Processing for one or more specified purposes (Article 9 (2) (a) GDPR), or when Personal Data have been 'manifestly made public by the data subject' (Article 9 (2) (e) GDPR).

Based on the specified purposes and envisioned use cases assessed in this DPIA there is a chance that Special Category Personal Data will be processed. For example, in the context of the use of TOPdesk by institutions for incident registration or for the registration of accidents/inappropriate behaviour in the context of social safety. For these purposes, institutions may want to process Special Category Personal Data related to, for example, health, sex life or sexual orientation. On the other hand, the use of TOPdesk as a Ticketing system for IT services would likely not require the Processing of Special Category Personal Data.

However, as this is an umbrella DPIA, the actual exceptions from Article 9(2) GDPR relied upon by institutions when Processing Special Category Personal Data cannot be identified in this DPIA. It is up to the institutions themselves to identify these legal exceptions and assess to what extent they apply. If institutions do not perform such assessments, there is a reasonable possibility that they will process their Special Category Personal Data unlawfully. Furthermore, institutions processing Special Category Personal Data as part of their use of TOPdesk must implement security measures to ensure adequate protection of such data – in addition to the measures applied to regular categories of Personal Data. TOPdesk offers several additional security measures such as applying Filters for different Operator groups (see §1.2.14.2), and making use of the private tab on a Person Card to register Special Category Personal Data (see §1.2.9). Both measures limit the amount of people with access to Special Category Personal Data, providing greater security.

If institutions Process Special Category Personal Data in TOPdesk without implementing additional security measures, it is likely that these Processing Activities will not comply with the GDPR. After all, the level of security must be appropriate to the risk posed by the Processing. The Processing of Special Categories of Personal Data involves high risks, meaning stricter security measures must be taken.

---

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

13. Purpose limitation

The principle of purpose limitation states that Personal Data may only be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; Further Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1) GDPR not be considered to be incompatible with the initial purposes" (Article 5 (1)(b) GDPR). Essentially, this means that the controller must have a specified purpose for which it collects Personal Data and can only process these data for purposes compatible with that original purpose.

According to the EDPB both purpose limitation and data minimisation principles are particularly relevant in contracts for online services, which typically are not negotiated on an individual basis. *"Technological advancements make it possible for controllers to easily collect and process more Personal Data than ever before. As a result, there is an acute risk that Data Controllers may seek to include general Processing terms in contracts in order to maximize the possible collection and uses of data, without adequately specifying those purposes or considering data minimisation obligations."*[55]

The predecessor of the EDPB, the Article 29 Working Party, has previously stated: *"The purpose of the collection must be clearly and specifically identified: it must be detailed enough to determine what kind of Processing is and is not included within the specified purpose, and to allow that compliance with the law can be assessed and data protection safeguards applied. For these reasons, a purpose that is vague or general, such as for instance 'improving users' experience', 'marketing purposes', 'IT-security purposes' or 'future research' will – without more detail - usually not meet the criteria of being 'specific'."*[56]

Data Controllers must be able to prove, based on Article 5(2) of the GDPR, that they comply with the principle of purpose limitation (accountability).

13.1 Further Processing by institutions

Whether institutions using TOPdesk comply with the principle of purpose limitation cannot be determined in this umbrella DPIA. This must be assessed and demonstrated by institutions themselves based on the factual purposes of their Processing Activities.

13.2 Further Processing by TOPdesk

Concerning the Processing Activities performed by TOPdesk as Controller, it cannot be determined with enough certainty whether the principle of purpose limitation is complied with based on the information provided by TOPdesk in the Privacy Statement on its

---

[55] 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, Adopted on 9 April 2019, p. 5-6. URL: https://edpb.europa.eu/sites/default/files/consultation/edpb_draft_guidelines-art_6-1-b-final_public_consultation_version_en.pdf.

[56] Article 29 Working Party Opinion 03/2013 on purpose limitation (WP203), p. 15–16,

website.[57] As described, this is due to the fact that TOPdesk's statement[58] on the Processing for its own purposes is not clearly reflected in TOPdesk's privacy statement on its website. This relates mainly to the Processing of message contents and website usage data for TOPdesk own purposes. It is not clear from the privacy statement whether TOPdesk also further Processes Personal Data collected as Processor for these own purposes. On the other hand:

- Both TOPdesk's[59] and SURF's[60] template DPA's do provide sufficient clarity as both explicitly state that TOPdesk may not (further) Process Personal Data collected as Processor for its own purposes
- The technical research did not reveal any further processing activities performed by TOPdesk as Controller.
- In e-mail communication with Privacy Company, TOPdesk has stated it does not Process Personal Data obtained as Processor for its own purposes as Controller.[61]

Thus, while most signs indicate that TOPdesk does not further Process Personal Data for its own purposes, this is not completely clear from the privacy statement.

---

[57] 'TOPdesk Privacy Statement', < https://www.topdesk.com/en/privacy-policy/> last accessed 10/09/2025.

[58] Statement made in communication between TOPdesk and Privacy Company. TOPdesk's fully reply is available at the request of SURF.

[59] TOPdesk template DPA, Article 3.2, v.2025.

[60] SURF template DPA, Art. 2.3.3.

[61] Statement made in communication between TOPdesk and Privacy Company. TOPdesk's fully reply is available at the request of SURF.

14. Necessity and proportionality

14.1 The concept of necessity

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. Proportionality means the invasion of privacy and the protection of the Personal Data of the Data Subjects is proportionate to the purposes of the Processing. Subsidiarity means that the purposes of the Processing cannot reasonably be achieved with other, less invasive means. If so, these alternatives have to be used.

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 controller needs to decrease the amount of Personal Data to what is necessary.

Therefore, essentially, the Data Controller may only process the Personal Data that are necessary to achieve the legitimate purpose but may not Process Personal Data it may do without. The application of the principle of proportionality is thus closely related to the principles of data protection from Article 5 GDPR.

This DPIA is an umbrella DPIA, because the processing activities performed with TOPdesk differ for each institution. As result, the necessity and proportionality of the Processing Activities performed by institutions with use of TOPdesk cannot be assessed in this DPIA. Institutions must make their own assessments based on their factual use of TOPdesk. The following paragraphs contain the conclusions that can be drawn based on this DPIA.

14.2 The concept of 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.

All Processing activities observed during testing were proportional except for the application logging. As described in 1.9.2 TOPdesk application logs, the log levels and the Personal Data logged at each level are not consistent. Usually logging systems define several ‘log levels’. A log level is a configuration of the logging system of an application. At each log level the logs have a different level of verbosity. It is common for log levels to range in verbosity from only reporting critical errors down to creating a verbose trace to debug the application. It is also common to log successful and failed authentication actions only in the moderately (and more) verbose log levels and to log content data only in the most verbose (trace) log level. The most verbose log level is usually only activated when system administrators are actively debugging an issue.

TOPdesk is not consistent in the implementation of the log levels of the application logs. Some database queries are logged including Personal Data and some with only field names.

Some of these queries are logged at the ‘debug’ log level, while others are logged at the ‘info’ log level. TOPdesk confirmed they don’t have a general policy on logging Personal Data at different log levels. This may result in logging of Personal Data that is unnecessary for the purpose of the logging. The default log level of the application logging is ‘debug’, after ‘trace’ the most verbose level.

Conclusion proportionality

he following general observations can be made in relation to the proportionality of Processing Personal Data in TOPdesk:

- Looking at the envisioned use cases assessed in this DPIA, the proportionality of Processing Personal Data in the context of recording incidents and accidents/inappropriate behaviour in the context of social safety will need to be carefully assessed. This is due to the sensitive context involved and the possibility that, as already mentioned in 12, Special Categories of Personal Data may (have to) be processed in this context.
- Prior to enabling optional additional functionalities in TOPdesk, such as integrating YouTube videos, enabling Google Analytics or using Ebbot Live Chat/the Ebbot AI Chatbot, it must be assessed whether the principles of necessity and proportionality are met. The proportionality of enabling these functionalities must be assessed in particular because, in principle, they are not necessary to achieve the purposes/envisioned use cases assessed in this DPIA.
- The application logging of TOPdesk is disproportionate.

14.3 The concept of subsidiarity

The key question is whether the same goals can be reached with less intrusive means. This question, again, must be answered by institutions themselves. This will depend, among other things, on whether institutions already use other means for the use cases within the scope of this DPIA, and the method of recording Personal Data in TOPdesk. If, for example, other means are already being used to record accidents/inappropriate behaviour in the context of social safety, it is likely to be too intrusive to also record this in TOPdesk. The assessment of whether other service management software is less intrusive then TOPdesk, must be done by comparing the DPIAs on both of them.

15. Data Subject Rights

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

The SURF template DPA includes the following relevant clauses in Article 3:

> *"3.1 The Processor shall provide the Controller with all necessary assistance and cooperation in fulfilling the obligations incumbent on the Parties under the GDPR and other applicable laws and regulations concerning the Processing of Personal Data. Insofar as such assistance relates to the Processing of Personal Data for the purpose of performing the Agreement, the Processor shall in any case provide the Controller with such assistance in relation to:*
> *[…]*
> *(vi) Complying with requests from Data Subjects;*
>
> *3.2 The provision of assistance and cooperation with regard to complying with requests from Data Subjects shall in any case be understood to mean the following obligations for the Processor:*
> *3.2.1 The Processor shall take all reasonable measures to ensure that the Data Subject can exercise his or her rights.*
> *3.2.2 If a Data Subject contacts the Processor directly in relation to the exercise of their rights, the Processor will not respond (in substance) unless expressly instructed otherwise by the Controller, but will immediately notify the Controller and request further instructions.*
> *3.2.3 If the Processor offers the Service directly to the Data Subject, the Processor is obliged to inform the Data Subject on behalf of the Controller about the Processing of the Data Subject's Personal Data in a manner that is consistent with the Data Subject's rights."*

The TOPdesk template DPA includes the following relevant clauses in Article 12:

> *"12.1 The Processor shall act in accordance with all reasonable instructions of the Controller and take all steps reasonably necessary to enable the Controller to respond to a 'Data Subject Request' as described in Chapter 3 of the GDPR.*
> *12.2 A request for cooperation shall be submitted in writing by the Controller to the Processor. The Processor shall respond to such a request without undue delay, unless prohibited by law.*
> *12.3 The Processor shall promptly and in any event as soon as possible communicate any Data Subject Request to the Controller and shall forward such request to the Controller and not handle it independently, unless otherwise required or prohibited by law or regulation.*

> *12.4 The Processor shall provide Personal Data in a structured, commonly used and machine- readable format without impeding the Controller in the transmission.*
> *12.5 The Processor shall provide the means by which the Controller can comply with the described requests. If these means prove inadequate, the Parties shall consult each other to find a solution to fulfil the described obligations."*

Both DPAs provide sufficient assurance to institutions and their Data Subjects that TOPdesk shall assist institutions when responding to Data Subject requests.

As part of this DPIA, the institution where the technical research was performed filed a Data Subject Access Request with TOPdesk in order to assess whether Data Subjects can indeed effectively exercise their rights. See 15.2 below for the results.

15.1 Right to information (transparency)

Data Subjects have a right to information (Articles 12-14 GDPR). This means that Data Controllers must provide them 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.

In relation to the Processing of their Personal Data due to the use of TOPdesk, Data Subjects must be informed about this by their institution. This can be done, for example, via a (specific) privacy statement. In part, institutions can derive the information to be provided from this DPIA. However, due to the nature of an umbrella DPIA, the specific information to be provided to meet the obligations from Articles 12-14 GDPR cannot be determined nor assessed.

Furthermore, TOPdesk also provides a significant amount of information about the Processing of Personal Data in TOPdesk. However, this information is accessible through TOPdesk's Knowledge Base which can be accessed after logging in to a TOPdesk environment, or which can be accessed by adding a redirect to an URL on the login page.[62] Since a Data Controller must meet its transparency obligations prior to any Processing Activities taking place, institutions must communicate this information to its Data Subjects prior to the creation of their TOPdesk User/Operator accounts. Based on the clauses in the template DPA's referenced above, TOPdesk is obliged to assist institutions in providing this information to Data Subjects.

An additional point to note is that TOPdesk requires institutions to actively sign up for notifications on changes to Sub-Processors, as mentioned in Involved Parties. Both template DPAs determine that TOPdesk will actively inform institutions on changes to Sub-Processors. It is unclear whether TOPdesk actually does so – or whether this first requires institutions to actively sign up for updates. The latter would mean that there is a risk that institutions do not (timely) inform Data Subjects on changes to Sub-Processors, meaning the institution's transparency obligations are not met. Moreover, this would mean (informed) consent to changes in Sub-Processors cannot be provided, as institutions must first be informed of such changes to do so.

---

[62] TOPdesk: Knowledge bank item KI 12939, A solution to make this redirect easier to implement is scheduled for Q1 2026

15.2 Right to access

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

As Data Controllers, institutions must comply with Access Requests filed by Data Subjects. TOPdesk must assist institutions in doing so, and they are obliged to do so based on the clauses in the respective DPAs referenced above.

As part of this DPIA a Data Subject Access Request was filed by the institution where the technical research was performed (see also Test: Access Request). During the procedure, Data Subjects/institutions filing a request on behalf of a Data Subject, receive an email that states it is required to reply to an automatic email sent by TOPdesk after filing a Data Subject request. This is made clear at the beginning and end of the automatic email.[63] However, TOPdesk processes the requests even without a reply of the Data Subject, despite this text in the email. This appears to be an unnecessary step in the procedure and requires Data Subjects to make extra effort to exercise their rights, which is not in line with the spirit of the GDPR. Further, the text of the e-mail contains hyperlinks (underlined in blue) and bold text – while the statement that Data Subjects should reply to the e-mail to have their request processed is written in plain text. Therefore, this call to action does not stand out and may go unnoticed by Data Subjects. To avoid any confusion TOPdesk has, during the course of this DPIA, removed the redundant text about the requirement to reply to the automatic email.

TOPdesk provided the HTTP logs from Cloudflare. These contained approximately 89% of the requests made and the information provided matched the traces from the testing. However, the provided loglines give a clear overview of the usage of the site: all relevant information is present in the provided loglines. The procedure TOPdesk developed to filter and analyse these log files, provides confidence in TOPdesk’s ability to answer future Data Subject Access Requests. Because of the delay in answering the request, no firewall logs from Cloudflare were provided. Therefore, these could not be assessed.

As described in Test: Access Request, the statutory response period was extended by two months because TOPdesk had not yet received the requested input from Cloudflare and Microsoft. TOPdesk ultimately received the responses within the additional two-month period and completed its response to the request within 1 month and 5 days. The content of these responses was not fully compliant, due to the missing information from Microsoft.

To prevent such delays in future, TOPdesk has taken the measures and made commitments, as described in Test: Access Request. They indicate that no similar future delays are to be expected. However, no amendments were made to the DPAs between TOPdesk and Cloudflare, respectively Microsoft. Therefore, there are no contractual guarantees that Cloudflare or

---

[63] The full (automated) reply by TOPdesk is available at the request of SURF.

Microsoft will enable TOPdesk to comply with Data Subject Requests within the statutory period of one month. Moreover, TOPdesk has stated in its final reply that it does not expect any delays or issues in obtaining additional information from Cloudflare or Microsoft. TOPdesk indicated that it has realized it can access and review most of the required information itself through the operator portals of the specific Sub-Processors. Furthermore, the company has established internal processes to respond more quickly to Data Subject Requests. In relation to Cloudflare, this is a reasonable expectation, based on the findings of the test Access Request and the measures implemented by TOPdesk.

15.3 Right to object

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

Insofar institutions perform any Processing Activities based on their legitimate interest(s), see also §11.211, they must facilitate the right to object. Based on the referenced clauses in the DPAs, TOPdesk is obliged to assist institutions, insofar reasonably possible, in facilitating such objections.

15.4 Right to rectification and erasure

Data Subjects have the right to have incorrect or outdated information corrected, to have incomplete information completed (Article 16 GDPR), and under certain circumstances to have Personal Data deleted (Article 17 GDPR).

TOPdesk facilitates institutions in complying with the right to rectification and erasure, and this is reflected in both DPAs. Moreover, institutions themselves can rectify Personal Data of Data Subjects and can delete (certain Personal Data of) Data Subjects from TOPdesk. Institutions must determine for themselves which Personal Data can, and which cannot, be rectified and/or deleted. The only exception is related to rectification and erasure requests in relation to Personal Data in log files; it is likely that institutions cannot (fully) comply with such requests.

If incorrect or incomplete Personal Data is processed in log files, this is due to an incorrectness or incompleteness in the source data, i.e. the Personal Data registered at account creation. By their very nature, log files record the Personal Data as it is recorded in the source data. Therefore, any request to rectify this data should be aimed at the source data, rather than the data in log files. Regarding erasure requests aimed at Personal Data in log files will usually not be applicable as none of the grounds in Article 17(1) GDPR apply. The purpose of Processing this Personal Data is to ensure the security of Personal Data, and the TOPdesk environment more broadly. The Personal Data recorded in log files will remain necessary for this purpose until these log files are deleted in line with the applicable retention policies. Moreover, rectifying or erasing Personal Data from log files would undermine this purpose and could compromise the protection of Data Subject's Personal Data required by the GDPR.

Part C: Description of the risks

This part concerns the description and assessment of the risks for Data Subjects. This part looks at both the risks connected to the key management as the risks connected to the Processing of Personal Data of the system administrators. The risks will subsequently be classified according to the likelihood they might occur, and the impact on the rights and freedoms of the Data Subjects when they do.

16. Risks

This part concerns the description and assessment of the risks for Data Subjects. These are the risks as found during testing and analysis and before taking mitigating measures. 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. The model this DPIA, based on “het Rijksmodel”, uses the risk categories and the risk model of the British Data Protection Authority, ICO. ICO lists the following main categories of risks:

- Loss of control over Personal Data
- Loss of confidentiality
- Impossible for the Data Subjects to exercise their rights
- Reidentification of pseudonymised Personal Data
- Unlawful Further Processing

These main categories give guidance to determining specific risks. By representing the risks encountered according to their potential impact on the rights and freedoms of Data Subjects, a picture of the high and low risks emerges. This is displayed in the risk graph developed by the UK regulator ICO, as follows:

Table 18: ICO Risk model

		Likelihood of harm		
		Remote	Reasonable possibility	More likely than not
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

This DPIA uses the following meanings of the “likelihood of harm” and the “severity of impact” to assess the risks:

Table 19: Definitions of likelihood:

Likelihood	Meaning
Very small	It is unlikely that this risk will occur
Reasonable possibility	It is conceivable that this risk will occur.
More likely than not	It is likely or certain that the risk will occur

Table 20: Definitions of impact

Impact	Meaning
Minimal impact	The consequences for the Data Subject have little or negligible impact on the data subject's rights and freedoms when the risk occurs
Some impact	The consequences for the Data Subject have a limited impact on the rights and freedoms of the Data Subject upon the occurrence of the risk
Serious harm (severe impact)	The consequences for the Data Subject have a substantial impact on the rights and freedoms of the Data Subject upon the occurrence of the risk

16.1 Identification of data protection risks

While conducting this DPIA, the following risks have been identified:

Table 21: risk overview

#	Risk	Type of risk	Likelihood	Impact
1.	Lack of policies regulating Personal Data in TOPdesk's log files	Loss of control	More likely than not	Serious impact
2.	Use of optional Sub-Processors	Loss of control – contracting based on TOPdesk template DPA	Reasonable possibility	Serious impact
3.	Active subscription required for updates on TOPdesk's Sub-Processors	Loss of control	Reasonable possibility	Serious impact
4.	Transfer of Personal Data via Cloudflare	Loss of control	More likely than not	Minimal impact
5.	ex-EEA access requests at Cloudflare	Loss of control	Remote possibility	Serious impact
6.	transfer of Personal Data via Microsoft	Loss of control	Remote possibility	Serious impact
7.	Automatic anonymisation fails for third Data Subjects	Loss of control	Reasonable possibility	Serious impact
8.	Untimely assistance by Cloudflare and Microsoft	Inability to exercise Data Subject rights	More likely than not	Serious impact
9.	Data invisible for caller	Inability to exercise Data Subject rights	Reasonable possibility	Serious impact
Risks applicable to institutions processing Special Category Personal Data with TOPdesk				
#	**Risk**	**Type of risk**	**Likelihood**	**Impact**
10.	Use of special categories of Personal Data in test or staging environment	Loss of confidentiality & Unlawful Further Processing	Reasonable possibility	Serious impact
11.	Processing Special Category Personal Data in TOPdesk	Loss of control	Reasonable possibility	Serious impact
12.	Insufficient audit logging on Special Categories of data	Loss of control	Reasonable possibility	Serious impact

Below is an explanation on the risks. These are divided into 'General risks', which may apply to all institutions using TOPdesk for the use cases assessed in this DPIA, and 'Risks associated with the processing of Special Category Personal Data with TOPdesk', as not all institutions will Process Special Category Personal Data when using TOPdesk.

16.2 General risks

16.2.1 Loss of control – lack of policies regulating Personal Data in TOPdesk's log files (risk # 1)

TOPdesk has indicated that they have a general policy to restrict storing Personal Data in logs to what is necessary. However, TOPdesk does not have specific policies on exactly which kinds of Personal Data are logged for each different log level. As a result of this, Personal Data is logged at log levels where that type of Personal Data is not expected nor needed to be logged.

The chance of this happening is more likely than not, as it is the factual situation. The harm for the rights and freedoms of the Data Subjects is serious, because the institution has no control over what data is logged at which log level, so attempts to minimize logging of personal data and storage of personal data in logfiles, may fail. Therefore, this risk is high.

16.2.2 Loss of control when contracting based on the TOPdesk template DPA – use of optional Sub-Processors of TOPdesk (risk # 2)

Institutions can choose to use the optional additional features in TOPdesk facilitated by Hello Ebbot AB, for Live Chat and AI Chatbot functionalities, and Insocial, which provides feedback solutions. If an institution chooses to do so, this must be reflected in the DPA between the institution and TOPdesk. The SURF template DPA specifically lists the applicable Sub-Processors. The TOPdesk template DPA, however, refers to a TOPdesk website for an overview of applicable Sub-Processors.[64] This website lists all factual and potential Sub-Processors of TOPdesk. Given this construction in the TOPdesk template DPA, it is not (immediately) clear which Sub-Processors are involved in the actual Processing of Personal Data of institutions' Data Subjects. Without clarity on which Sub-Processors are factually involved in the Processing, there is insufficient control over that Processing.

The likelihood of this risk causing harm to the rights and freedoms of the Data Subject is reasonable; the list is available on the website, so institutions do have means to remain in control, however it would require institutions to have in place a policy/procedure requiring active monitoring of that website. Loss of control happens when the data controllers don't properly inform Data Subjects about the Processing of their Personal Data by Sub-Processors. Without proper information they are not put in a position where they can exercise effective control over their Personal Data which may lead to serious harm. Given the reasonable likelihood, combined with the serious impact, this risk is high.

16.2.3 Loss of control – active subscription required for updates on TOPdesk's Sub-Processors (risk # 3)

Institutions must actively sign up via a TOPdesk website to receive updates about changes to Sub-Processors. Institutions that do not (notice that they must) actively sign up will not be informed about such changes and, therefore, cannot inform their Data Subjects who, in turn, run the risk of losing control over their Personal Data processed by Sub-Processors. Moreover, it is not clear how consent for changes in Sub-Processors is to be provided by institutions that do not actively sign up to updates. If TOPdesk does not ask institutions for

---

[64] TOPdesk template Data Processing agreement, v. 2025, p. 10.

consent in such cases, this qualifies as a violation of both the SURF template DPA and the TOPdesk template DPA.

There is a reasonable possibility of this occurring as institutions must themselves notice the requirement to be able to actively sign up to updates. Without proper information, the impact is that Data Subjects are not put in a position where they can exercise effective control over their Personal Data which may lead to serious harm. The overall risk is high.

16.2.4 Loss of control – transfer of Personal Data via Cloudflare not reflected in DPA (risk # 4)

According to the TOPdesk template DPA and the SURF template DPA assessed in this DPIA, no transfer of Personal Data occurs through the use of TOPdesk by institutions. However, the technical research shows that IP addresses of Data Subjects are transferred to Cloudflare in the US in the context of DDoS protection. Moreover, the DPA between TOPdesk and Cloudflare mentions this transfer and TOPdesk has indicated that this transfer cannot technically be prevented. The transfer constitutes a violation of the DPA between TOPdesk and an institution and leads to a loss of control over Personal Data for Data Subjects.

The chance of this happening is more likely than not, as the technical research shows the transfer factually occurs. The impact for Data Subjects is minimal, however, because the transfer only entails IP addresses without any context. These cannot be used, for example, to discriminate against or exclude Data Subjects. However, as this transfer is not documented in the DPA there is a violation of the GDPR and DPA. This, in turn, may lead to a loss of control over the transferred Personal Data. As the GDPR and DPA are both intended to safeguard the rights and freedoms of Data Subjects, an absence of such safeguards leads to risks for the rights and freedoms of Data Subjects. The associated risk is low.

16.2.5 Loss of control – ex-EEA access requests at Cloudflare (risk # 5)

Cloudflare processes the list of IP-addresses Cloudflare is blocking, worldwide. This list of IP-addresses may contain the IP-addresses of TOPdesk end-users, for example when they are infected with malware. The worldwide processing means this list falls under the scope of non-EU laws and is therefore subject to non-EU procedures of law enforcement access to the data. Cloudflare monitors such access in their transparency report. Additionally, Cloudflare has canary provisions in their transparency report, which TOPdesk monitors.

Because of the rarity of legal requests like these, and because of only a very small subset of the TOPdesk end users being included in this list, the chance of this happening, is very small. When it happens, however, it causes a loss of control for Data Subjects which may lead to serious harm to their rights and freedoms, like prosecution in a non-EEA country. As such, this risk is low.

16.2.6 Loss of control – transfer of Personal Data via Microsoft (risk # 6)

TOPdesk implements encryption for the data stored at Microsoft, in combination with Microsoft ‘Customer-managed keys’, backed by a hardware security module. However, this setup does not provide full control over the keys and data by TOPdesk. While there are no indications that the use of TOPdesk by institutions leads to the transfer of Personal Data via Microsoft, TOPdesk has stated that this transfer cannot be technically excluded.

Moreover, the DPA between TOPdesk and Microsoft does not exclude such transfers and lacks a canary clause for when an ex-EEA entity requests data at Microsoft, combined with a gagging-order. Therefore, there is a risk that such transfer takes place which would lead to a loss of control over Personal Data for Data Subjects. Because of the rarity of non-regular transfers, the chance of this happening, is very small. When it happens, When it happens, it causes a loss of control for Data Subjects, which may lead to serious harm to the rights and freedoms of the Data Subject. Therefore, this risk is low.

16.2.7 Loss of control – anonymisation does not anonymise data about Data Subjects mentioned in cards (risk # 7)

The automated data anonymisation process only recognises Personal Data from the linked persons cards. If the card that needs to be anonymised contains data about a Data Subject that is not in a linked person card, then this data is not anonymised. To avoid storage of this Personal Data beyond the retention policies, these cards either need to be sanitized manually or need to be deleted altogether. A failure to anonymise or delete the cards, leads to storage of Personal Data outside the retention policy of the institution.

Accurately assessing this risk is difficult because it is linked to the possibility that an institution has not implemented sufficient measures, meaning it is unclear whether additional steps are needed to fully anonymize Personal Data. Since this cannot be accurately evaluated based on this DPIA, the possibility is considered reasonable. The potential impact of this risk is easier to assess. If the risk materializes, Personal Data will be stored longer than necessary, which violates the principle of storage limitation. Violating a basic GDPR principle has a serious impact on the rights and freedoms of Data Subjects. Therefore, this risk is high.

16.2.8 Inability to exercise Data Subject Rights – untimely assistance by Cloudflare and Microsoft based on the DPA (risk # 8)

As part of this DPIA a Data Subject Access Request was filed with TOPdesk by the institution where the technical research was performed. The Access Request also contained questions on the Processing by Cloudflare and Microsoft. Therefore, TOPdesk sought assistance from Cloudflare and Microsoft to comply with the request. However, neither Cloudflare nor Microsoft provided a timely response. Due to this, TOPdesk had to extend the deadline to comply with the request by 2 months, per Article 12(3) GDPR.

Eventually Cloudflare provided TOPdesk with a procedure to download and analyse the logs themselves. However, by the time this procedure was in place, a part of the logs were already deleted because of a retention period of 30 days. Because this procedure is now in place, TOPdesk will be able to fully comply with these requests on Cloudflare logs within 30 days.

Well after the extended deadline of 2 months, TOPdesk was able to confirm with Microsoft that the requested logfiles do not contain the IP-addresses.

The chance of this risk occurring is more likely than not: as evidenced during the DPIA, TOPdesk was not able to meet the 2-month deadline due to untimely assistance by its Sub-Processors. Failure to meet the deadline results in serious harm to the rights of the Data Subject. Therefore, this risk is high.

16.2.9 Inability to exercise Data Subject Rights – data ‘invisible to a Caller’ (risk # 9)

When responding to a Call, Operators can choose to have their answer be ‘invisible to a Caller’ which allows for internal communication relating to the Call. These notes are linked to a caller and therefore are Personal Data and subject to Data Subject Rights. However, the institution needs to actively provide this data to the Data Subject, because it is inaccessible from the self-service portal available to the Data Subject. When the institution lacks a proper procedure to also provide these data, the Data Subject cannot exercise their rights.

When an institution receives a data subject access request, the standard response for TOPdesk would be to refer back to the self-service portal, because normally all data is available there. However, when the card contains answers that are ‘invisible to Caller’, the privacy officer, support officer or system administrator answering the question, must manually provide the invisible answers. So, they must be aware of this and need to have a procedure to do so. Because this is not obvious when implementing TOPdesk, there is a reasonable possibility this data is not provided. The harm for the Data Subject when the data is not provided is serious, because then the Data Subject cannot properly exercise their (fundamental) rights under the GDPR. Therefore, this risk is high.

16.3 Risks applicable to institutions processing Special Category Personal Data with TOPdesk

Note that the risks described below only apply to the extent that an institution uses TOPdesk to Process Special Category Personal Data.

16.3.1 Loss of confidentiality & Unlawful Further Processing – use of Special Categories of Personal Data in test or staging environment (risk # 10)

If institutions use a copy of their production environment (which may include Special Categories of Personal Data) to set up a test or staging environment, there is an increased chance of Personal Data Breaches occurring due to the fact that institutions, in general, are less strict when applying their information security policies to test or staging environments. For example, authorisations are more readily granted in these environments, meaning individuals who would not normally have access to (Special Category) Personal Data in the production environment may gain access to it via the test or staging environment. Moreover, creating an entire copy of a production environment in a test or staging environment creates a second attack surface which increases the likelihood of a Personal Data Breach occurring. There is a significant chance that institutions wishing to set up a test or staging environment will create a copy of their (entire) production environment since:

- the default set of synthetic data that is available on request at TOPdesk may not be sufficient. While the synthetic data is not tailored for the custom processes the organisation has defined and therefore may have limited usability; and
- manually creating database queries to generate synthetic data is a relatively labour-intensive process for institutions.

Copying (Special Category) Personal Data from a production environment to a test or staging environment qualifies as a further Processing Activity (ex. Article 6(4) GDPR) and must therefore be compatible with the purpose for which the Personal Data are initially collected taking into account several factors. However, if institutions do not properly inform Data Subjects of this Further Processing, or if, for example, the information security policy is applied less strictly to the Personal Data in the test or staging environment, this Further Processing activity is highly likely to be unlawful. This holds true especially in case the

Personal Data includes Special Category Personal Data, because the threshold for compatibility is significantly higher in such cases and additional measures *must* be taken.

TOPdesk states, in reaction to this risk:

> "Acceptance environments are typically only used by application managers that already have a lot of permissions. When other users are granted access to the acceptance environment, database filters still apply and limit access to sensitive data. When TOPdesk is used in accordance with best practices, there is a separate permission group for accessing sensitive personal data, which you don't need to grant for colleagues to run an effective test.
> Lastly, in all cases the data remains within the same organisation. These are colleagues that will typically be bound by a confidentiality agreement and also have an interest in keeping internal data internal."

However, observations during testing showed that application managers were restraining themselves less in the testing environment then they would have in production. Therefore, Special Categories of Data that would not have been accessible by them in the production environment might be accessible in the testing environment.

Because it was discovered during the technical research that the institution where the research was performed, processed production data containing Special Categories of Data in a testing environment, it is assumed that there is a reasonable possibility that other institutions do so as well. The degree of harm when Special Categories of Data are Processed in the testing environment, is serious because this Data is unlawfully Processed. Therefore, this risk is high.

16.3.2 Loss of control – Processing Special Category Personal Data in TOPdesk (risk # 11)

Institutions can process all types of Personal Data in TOPdesk, including Special Category Personal Data. Given the envisioned use cases assessed in this DPA – specifically concerning the use of TOPdesk by institutions for incident registration or for the registration of accidents/inappropriate behaviour in the context of social safety – there is a chance that Special Category Personal Data will be processed. Also, the institution can configure 'Attentions' connected to persons, like 'is visually impaired'. As a Controller, an institution must determine for itself whether they can rely on one of the exceptions in Article 9(2) GDPR to legitimise the Processing. Furthermore, if an institution intends to process Special Category data in TOPdesk, this must be adequately reflected in the DPA between the institution and TOPdesk to provide adequate control for Data Subjects. Not all institutions use TOPdesk for processes that entail the Processing of Special Category of data, but some do. When they do – and none of the exceptions in Article 9(2) GDPR apply – this risk materialises.

In order to assess the likelihood of this risk materializing, the likelihood that an institution will fail to perform the required compliance work must be determined. Based on this DPIA, no substantiated statement can be made in this regard, although anecdotal evidence of insufficient governance of special categories of data was found during the technical investigation. For the purpose of this risk assessment, it is therefore assumed that there is a reasonable possibility that institutions will fail to perform all the required compliance work.

When this happens, the Processing is likely to be unlawful and in violation of the GDPR which leads to serious harm for the rights and freedoms of the Data Subject. Therefore, this risk is high.

16.3.3 Loss of control – insufficient audit logging on Special Categories of data (risk # 12)

In addition to the 'standard' configured logs, institutions can also define an audit trail (with log entries) within their own TOPdesk environment. For processes that are likely to contain Special Categories of Personal Data an extensive audit trail, containing who has accessed the data, is needed. This must be implemented by institutions as custom events to include in the audit trail. A failure to do so, leads to loss of control over who has accessed Special Category Data. This risk applies only insofar Special Category Personal Data is Processed by an institution in TOPdesk as the nature of the other data in TOPdesk is not as sensitive: it most likely does not contain exact location data, assessments of study or work-related performance, or other sensitive information. Therefore, the absence of audit logging when processing regular Personal Data in TOPdesk does not pose significant risks, and additional logging would in fact be disproportionate.

These logs need to be configured manually, depending on what fields contain data that requires extra logging. Because configuring this is not standard when configuring the workflows in TOPdesk, there is a reasonable possibility of the institution not implementing this. The harm for the Data Subject when this part of the audit trail is absent is serious, because Special Categories of data are processed without sufficient oversight over who has accessed it, which may lead to unlawful processing. Therefore, this risk is high.

16.4 Risk matrix

By representing the risks encountered according to their potential impact on the rights and freedoms of Data Subjects, a picture of the high and low risks associated with Processing Personal Data in TOPdesk emerges. This is displayed in the risk graph developed by the UK regulator ICO.

Table 22: Risk matrix

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

Part D: mitigating measures

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

17. Risk mitigating measures

17.1 Measures to be taken to mitigate privacy risks

The table below show the high data protection risks for Data Subjects, with the mitigating measures the educational institution and TOPdesk. The measures for the risks that were initially low already are *italic*.

Table 23: Mitigating measures

#	Risk	Measures Institution	Measures TOPdesk	Risk after mitigation	Status of TOPdesk measure
1.	Loss of control – lack of policies regulating Personal Data in TOPdesk's log files	None	Create and implement logging Policy describing what kind of Personal Data is logged at each log level.	Low	TOPdesk has created a logging policy which needs to be implemented by all departments. The deadline for this is Q4 2026.
2.	Loss of control when contracting based on the TOPdesk template DPA – use of optional Sub-Processors of TOPdesk	Ensure the DPA between the institution and TOPdesk reflects the Sub-Processors that are factually engaged	Define optional Sub-Processors within table on SaaS website.	Low	Since 06-10-2025 TOPdesk's SaaS information page lists which Sub-Processors are optional and informs customers that they can find the applicable Sub-Processors in their Main Agreement. Due to this implemented measure, the risk is now low.

#	Risk	Measures Institution	Measures TOPdesk	Risk after mitigation	Status of TOPdesk measure
3.	Loss of control – Active subscription required for updates on TOPdesk's Sub-Processors	None	Actively inform all Controllers on changes to Sub-Processors and ask for consent for each change.	Low	On 09-10-2025 TOPdesk adjusted its policy. Now, all registered SaaS Main Contact Persons receive a notification of a new Sub-Processor by default. Due to this implemented measure, the risk is now low.
4.	Loss of control – Transfer of Personal Data via Cloudflare not reflected in DPA	*Ensure that the transfer of Personal Data via Cloudflare is properly reflected in the DPA and complies with Chapter V GDPR*	*Amend the TOPdesk template DPA to reflect the transfer of Personal Data to Cloudflare*	Low	This risk is already low, so no measures are mandatory. However, TOPdesk will implement this measure by Q1 2026.

#	Risk	Measures Institution	Measures TOPdesk	Risk after mitigation	Status of TOPdesk measure
5.	Loss of control – ex-EEA access requests at Cloudflare	*None*	*Monitor possible disclosures*	Low	This risk is low, so no measures are mandatory. However, TOPdesk will continue to monitor possible disclosures by Cloudflare.
6.	Loss of control – transfer of Personal Data via Microsoft	*None*	*Monitor possible disclosures*	Low	This risk is low, so no measures are mandatory. However, TOPdesk will continue to monitor possible disclosures by Microsoft.

#	Risk	Measures Institution	Measures TOPdesk	Risk after mitigation	Status of TOPdesk measure
7.	Loss of control – Automatic anonymisation fails for third Data Subjects	Implement one of, or a combination of: • A policy to not include Personal Data about third persons in the free text fields of a card • A policy to manually anonymise the fee text fields of a card • A policy to not anonymise but delete cards after their retention period	None	Low	Not applicable
8.	Inability to exercise Data Subject rights – Untimely assistance by Cloudflare and Microsoft	None	Implement a procedure to provide personal data from the logfiles of Cloudflare.	Low	On 17-09-2025 TOPdesk has implemented a procedure for providing personal data from the logfiles of Cloudflare. Due to this measure, the risk is now low.
9.	Inability to exercise Data Subject rights – Data invisible for Caller	Implement procedure to include invisible answers in the answers to Data Subject requests.	None	Low	On 18-11-2025 TOPdesk has added to the best practices in the knowledgebase the need of implementing this procedure.

Measures for institutions Processing Special Category Personal Data with TOPdesk

#	Risk	Measures Institution	Measures TOPdesk	Risk after mitigation	Status of TOPdesk measure

#	Risk	Measures Institution	Measures TOPdesk	Risk after mitigation	Status of TOPdesk measure
10.	Loss of confidentiality & unlawful Further Processing – Use of Special Categories of Personal Data in test or staging environment	Make use of option to run database queries to replace Personal Data from production environment with synthetic data prior to copying the data to a test or staging environment	Offer the possibility to automatically remove the private and contract tab from the cards when transferring production data to a test or staging environment.	Low	TOPdesk has indicated that they are working on implementing this measure. Deadline is Q2 2026. Additionally, on 18-11-2025 TOPdesk has added to the best practices in the knowledgebase the need to implement this procedure.
11.	Loss of control – Processing Special Category Personal Data in TOPdesk	Perform the proper compliance work prior to Processing Special Category Personal Data in TOPdesk to ensure the institution can rely on one of the exceptions in Article 9(2) GDPR. When Processing Special Category Personal Data in TOPdesk, ensure that this is properly reflected in the DPA with TOPdesk.	Create or update a knowledge item for Institutions that provides information and best practices on processing special category data in TOPdesk.	Low	TOPdesk expects this measure to be implemented by end of Q4 2025.

#	Risk	Measures Institution	Measures TOPdesk	Risk after mitigation	Status of TOPdesk measure
		Don’t configure (medical) conditions in Attentions, but relevant actions for an operator to take. When registering Special Category Personal Data of a Data Subject, make use of the private tab on the Person card in the Supporting Files module (see §1.2.9).			
12.	Loss of control – insufficient audit logging on Special Categories of data	In absence of TOPdesk’s implementation of additional logging on access and modification of the private tab: Implement audit logging on accessing cards of processes likely to contain Special Categories of data. After TOPdesk’s implementation of additional logging on access and modification of the private tab: make use of the private tab on Person Cards to Process Special Category Data.	Implement additional audit logging: log who opened which card when and add this option to custom log actions.	Low	TOPdesk will implement additional logging on access and modification of the private tab on the Person card by default. This is scheduled for Q1 2026.

17.2 Assessment of risk after measures

If any of the residual risks after implementing the mitigative measures is ‘high’ then a prior consultation at the data protection authority is obliged. Based on the analysis, after implementing the mitigative measures, only low residual risks remain. Therefore, no prior consultation is needed.

18. Conclusion

This DPIA has identified nine high risks and three low risks to the rights and freedoms of Data Subjects.

These risks are partly due to the way institutions (will likely) use TOPdesk, and partly due to the design of TOPdesk itself. Three of the high risks are linked to the possibility that an institution Processes Special Category Personal Data in TOPdesk; if an institution does not do this, these three risks do not apply. Measures have been proposed for all risks, including the three low-level risks. Seven of these measures apply to institutions and ten to TOPdesk.

Implementing these measures will mitigate all high risks, leaving only low residual risks. In that case, no prior consultation with the Data Protection Authority is required. Although it is not strictly necessary to mitigate low risks, it is recommended as the measures are relatively easy to implement and strengthen Data Subjects' rights and freedoms.

> **Update 12/12/2025:** While the DPIA was being carried out, TOPdesk already implemented several measures to mitigate identified risks. More specifically, TOPdesk has already taken measures for four high risks (#2, 3, 8, 9) and implemented measures for all low risks. One high risk only needs measures from the institution. As such, at time of writing, four high risks remain. All of these risks have a timeline for implementing the measures. Therefore, institutions can continue using. If the remaining high risks are mitigated, no prior consultation with the Data Protection Authority is required. SURF will publish an update on this DPIA with a conclusion on the implementation of the remaining measures in 2026.

Annex 1: Additional information on the different TOPdesk modules

Action management module

Table 24 Types of Events to build automations[65]

Events	Action
New Card	Institutions can configure Actions that are triggered when a new Card is created by a Caller or Operator. For example, institutions can configure an Event-and-Action combination that automatically sends an email to a Caller that has created a new Call Card.
Edit Card	Institutions can create an Event that is triggered after a Caller or Operator edits information contained in a Card. This Event will be triggered when the value of a field is changed, for example from empty to any value, or from ‘value A’ to ‘value B’. This can be used, for example, to notify Operators when a Caller has provided additional information about a request. Or, vice versa, to notify a Caller when an Operator has responded/provided additional information to a Card.
Delete Card	Institutions can set up an Action that is triggered when a User or Operator deletes a Card. For example, a deletion notification may be sent to the Caller that initially created a Card.
Move to this Card type	Institutions can set up an Action for when an Operator changes a Card from a certain Card type to another one. For example, when a Call Card is escalated from first line to second line, or when a Card is archived.
Move from this Card type	
Card date	Institutions can create an Action that is triggered based on Card dates, such as the target date, time of registration, or date of completion. This can be used, for example, to send an automatic reminder to an Operator if a Card has not been responded to after a certain amount of time, or if you want to notify a manager that a contract will expire in a month.

Table 25: Available types of Actions that can be set up in TOPdesk[66]

Types of Actions	Explanation
Automated Actions (Action Sequence)	An Automated Action, based on API requests, is integrated in the Action Sequences system. Responses to previous requests in the series can be (re)used. Institutions can send a request from TOPdesk to another program (another

---

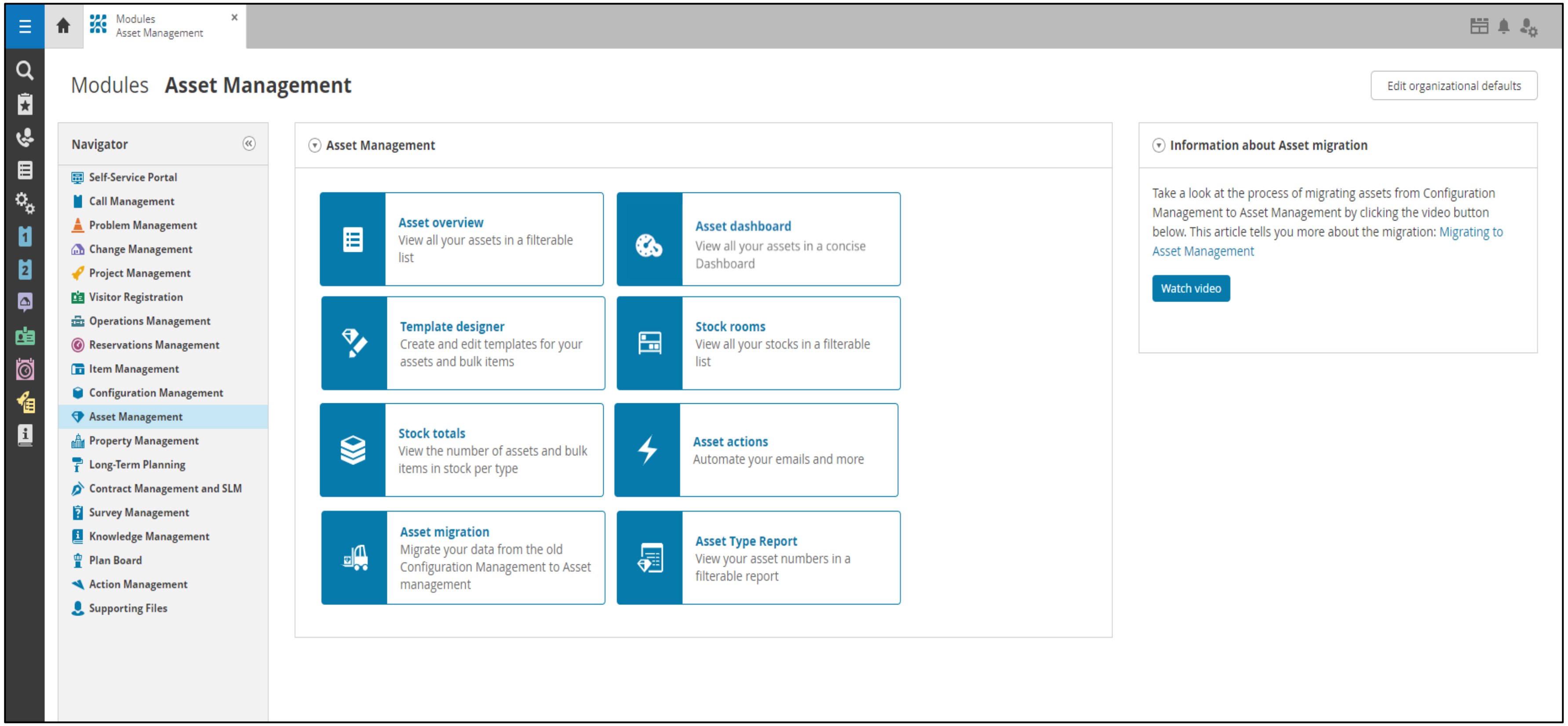
[65] See https://docs.topdesk.com/en/Events-that-trigger-Actions.html last accessed 28 March 2025.

[66] https://docs.topdesk.com/en/available-types-of-Actions.html last accessed 28 March 2025.

	TOPdesk environment or a different program), get a response back, and use the content of that response in a follow-up request. This way you can create an integration with almost any software that has a REST API.
Emails	Institutions can send an email to a Caller, Operator or third party when a specific Event occurs. To do so, an email Action must be created using a template email message and by defining the sender and recipient(s). Institutions can choose to fully automate email delivery or make it possible to edit email messages before they are sent.
Generate document	For Automated Actions, Generate document is an option to create a PDF file based on a template, information in the request body, and/or information from a Card.
Log Actions	With this type of Action, institutions can track changes made to certain Fields on a Card or when a Card is edited in general. For example, an Action can be configured to automatically register Card changes in a log entry by registering the old and new value.

Asset management module

Screenshot 1: Asset Management module[67]



Asset overview View all your assets in a filterable list

Asset dashboard View all your assets in a concise Dashboard

Template designer Create and edit templates for your assets and bulk items

Stock rooms View all your stocks in a filterable list

Stock totals View the number of assets and bulk items in stock per type

Asset actions Automate your emails and more

Asset migration Migrate your data from the old Configuration Management to Asset management

Asset Type Report View your asset numbers in a filterable report

Take a look at the process of migrating assets from Configuration Management to Asset Management by clicking the video button below. This article tells you more about the migration: Migrating to Asset Management

Table 26: Overview of available Widgets in TOPdesk's Asset Management module[68]

General Widget: **Provides an ID and numbering for the Asset**	**Dataset Widget:** **Creates customised columns and rows for multiple entries of data**

---

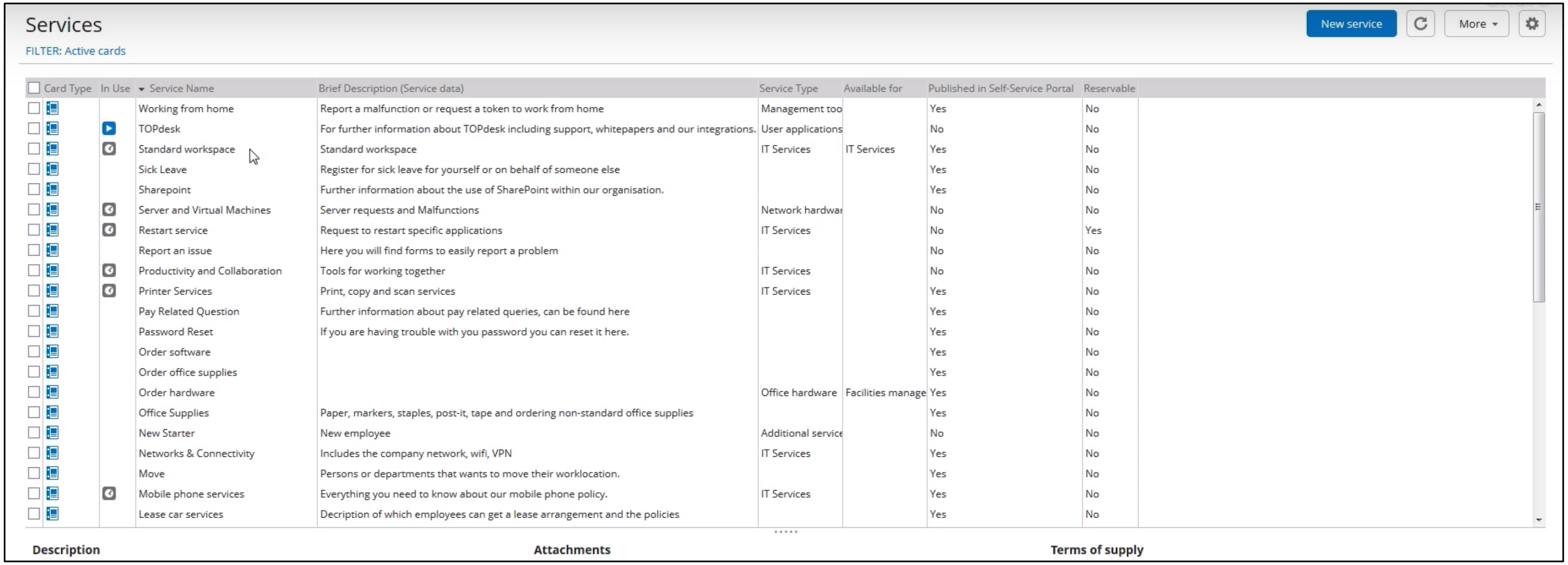
[67] https://docs.topdesk.com/en/the-asset-management-module-page.html last accessed 28 March 2025.

[68] https://docs.topdesk.com/en/designing-templates-for-assets.html last accessed 28 March 2025.

History Widget: Shows both present and past changes that have been made to an Asset	Reservations Widget: Manages how Assets are reserved. Use this widget to make Assets available in the Self-Service Portal.
Assignment Widget: Assigns locations and persons to the Asset	Documents Widget: Displays documents uploaded to the Asset.
Relationship Widget: Creates and shows an Asset's links to other Assets	Stock Widget: Link Assets to a stock to better manage your inventory.
Fieldset Widget: Creates customised fields that you can use to characterize information through various formatting options	Web content Widget: Shows web content from other web-based sources on the Asset Card.
Relationships grid Widget: Shows a summary of assets of a specific linked Asset type. For example, use this widget to show the amount of available licences on a software Asset Card.	Hyperlink Widget: Shows one or multiple clickable links on the Asset Card.

Operator section: available services

Screenshot 2: Example of a Service Catalogue in the Operator section of TOPdesk[69]



Services

FILTER: Active cards

☐	Card Type	In Use	Service Name	Brief Description (Service data)	Service Type	Available for	Published in Self-Service Portal	Reservable
☐	▤		Working from home	Report a malfunction or request a token to work from home	Management too		Yes	No
☐	▤	▶	TOPdesk	For further information about TOPdesk including support, whitepapers and our integrations.	User applications		No	No
☐	▤	◀	Standard workspace	Standard workspace	IT Services	IT Services	Yes	No
☐	▤		Sick Leave	Register for sick leave for yourself or on behalf of someone else			Yes	No
☐	▤		Sharepoint	Further information about the use of SharePoint within our organisation.			Yes	No
☐	▤	◀	Server and Virtual Machines	Server requests and Malfunctions	Network hardwar		No	No
☐	▤	◀	Restart service	Request to restart specific applications	IT Services		No	Yes
☐	▤		Report an issue	Here you will find forms to easily report a problem			No	No
☐	▤	◀	Productivity and Collaboration	Tools for working together	IT Services		No	No
☐	▤	◀	Printer Services	Print, copy and scan services	IT Services		Yes	No
☐	▤		Pay Related Question	Further information about pay related queries, can be found here			Yes	No
☐	▤		Password Reset	If you are having trouble with you password you can reset it here.			Yes	No
☐	▤		Order software				Yes	No
☐	▤		Order office supplies				Yes	No
☐	▤		Order hardware		Office hardware	Facilities manage	Yes	No
☐	▤		Office Supplies	Paper, markers, staples, post-it, tape and ordering non-standard office supplies			Yes	No
☐	▤		New Starter	New employee	Additional service		No	No
☐	▤		Networks & Connectivity	Includes the company network, wifi, VPN	IT Services		Yes	No
☐	▤		Move	Persons or departments that wants to move their worklocation.			Yes	No
☐	▤	◀	Mobile phone services	Everything you need to know about our mobile phone policy.	IT Services		Yes	No
☐	▤		Lease car services	Decription of which employees can get a lease arrangement and the policies			Yes	No

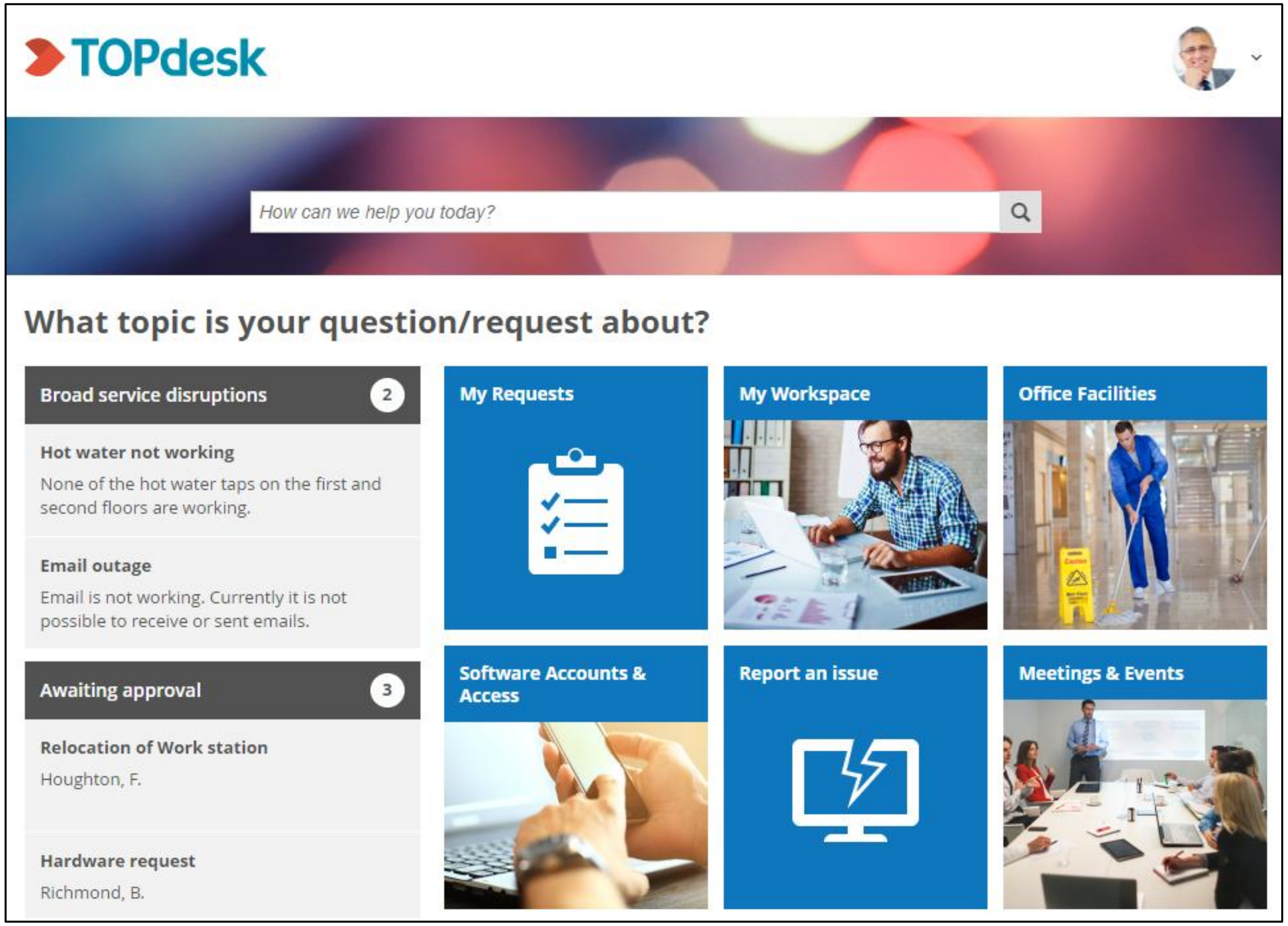
Description **Attachments** **Terms of supply**

---

[69] https://docs.topdesk.com/en/service-catalogue-in-topdesk.html last accessed 28 March 2025

Self-Service Portal

Screenshot 3: Example of a customised TOPdesk Self-Service Portal[70]



What topic is your question/request about?

Broad service disruptions 2

Hot water not working
None of the hot water taps on the first and second floors are working.

Email outage
Email is not working. Currently it is not possible to receive or sent emails.

Awaiting approval 3

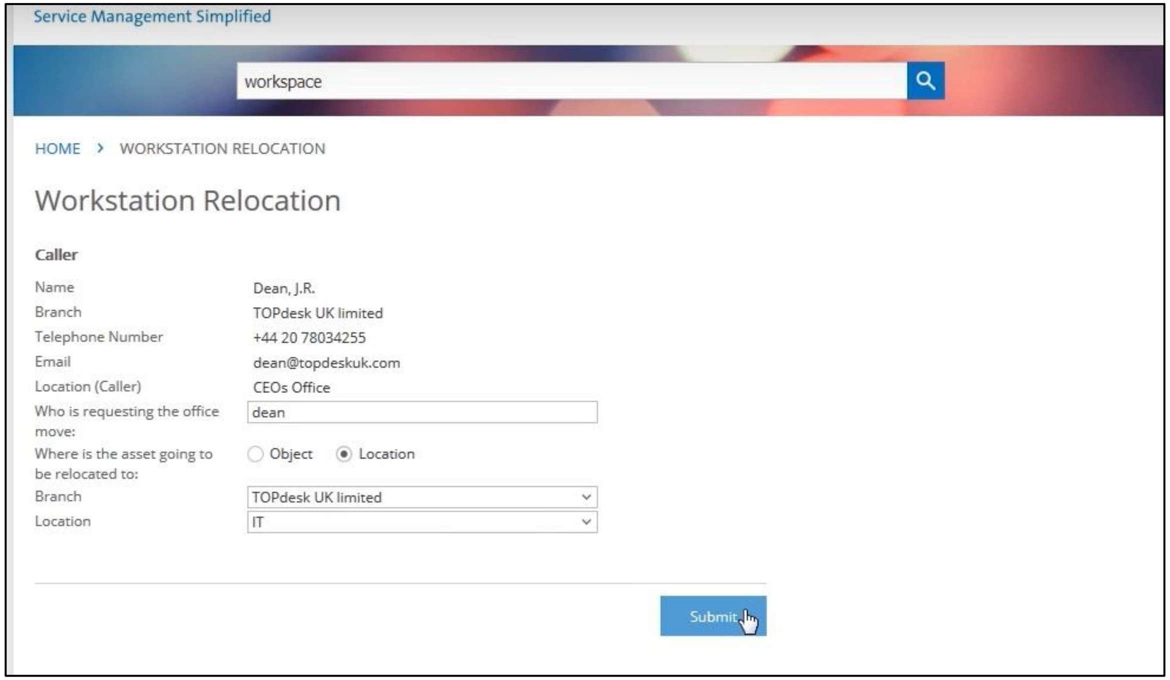
Relocation of Work station
Houghton, F.

Hardware request
Richmond, B.

---

[70] https://docs.topdesk.com/en/using-the-self-service-portal.html last accessed 28 March 2025.

Screenshot 4: Creating a Call through the SSP[71]



Workstation Relocation

Caller

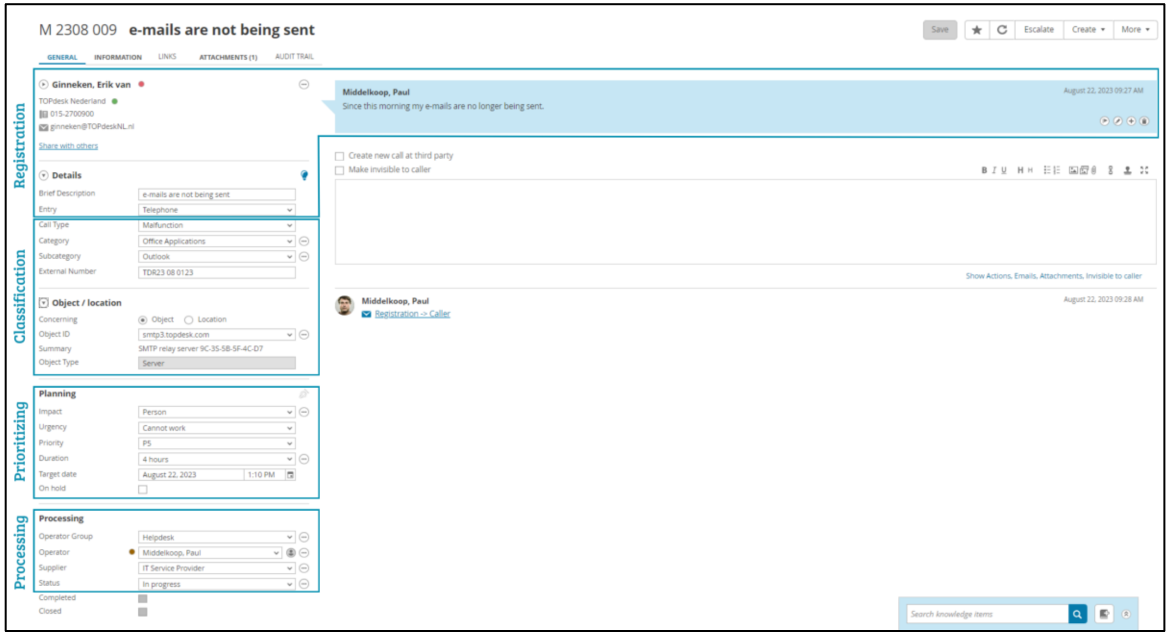
Name	Dean, J.R.
Branch	TOPdesk UK limited
Telephone Number	+44 20 78034255
Email	dean@topdeskuk.com
Location (Caller)	CEOs Office
Who is requesting the office move:	dean
Where is the asset going to be relocated to:	○ Object ● Location
Branch	TOPdesk UK limited
Location	IT

---

[71] https://docs.topdesk.com/VA2023R2/en/the-self-service-portal.html last accessed 28 March 2025.

Call Management module

Screenshot 5: Example of a Call[72]



M 2308 009 **e-mails are not being sent**

Ginneken, Erik van
TOPdesk Nederland
015-2700900
ginneken@TOPdeskNL.nl

Details

Brief Description	e-mails are not being sent
Entry	Telephone
Call Type	Malfunction
Category	Office Applications
Subcategory	Outlook
External Number	TDR23 08 0123

Object / location

Concerning	● Object ○ Location
Object ID	smtp3.topdesk.com
Summary	SMTP relay server 9C-35-5B-5F-4C-D7
Object Type	Server

Planning

Impact	Person
Urgency	Cannot work
Priority	P5
Duration	4 hours
Target date	August 22, 2023 1:10 PM
On hold	☐

Processing

Operator Group	Helpdesk
Operator	Middelkoop, Paul
Supplier	IT Service Provider
Status	In progress
Completed	☐
Closed	☐

Middelkoop, Paul August 22, 2023 09:27 AM
Since this morning my e-mails are no longer being sent.

☐ Create new call at third party
☐ Make invisible to caller

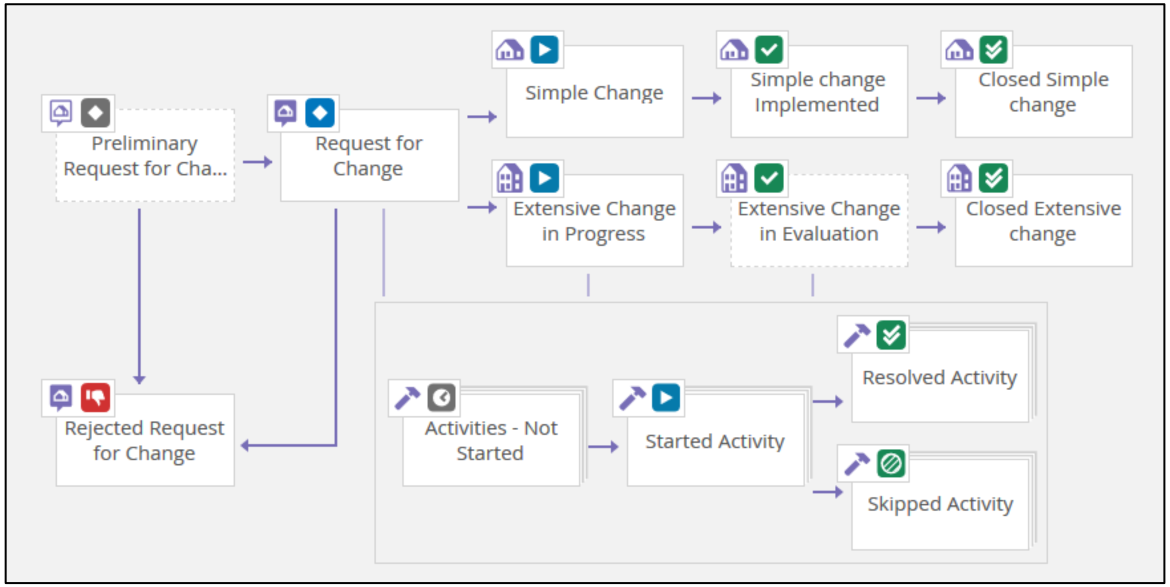
Middelkoop, Paul August 22, 2023 09:28 AM
Registration -> Caller

---

[72] https://docs.topdesk.com/VA2023R2/en/the-self-service-portal.html last accessed 28 March 2025.

Change Management module

Figure 1. Module diagram Change Management



In TOPdesk, changes comprise a number of phases. The first phase is dependent on whether RfC's must be first authorised by managers or not. This is configured through the Module Settings for Change Management. If such prior authorisation is enabled, the first phase is called the Preliminary Request for Change phase; if such authorisation is not enabled, the first phase is called the Request for Change phase. As such the phases are:

- Phase 1, option 1: Preliminary request for change phase: a preliminary request for change (PRfC) can be submitted either by Users via the Self-Service Portal or by Operators via the Operator's Section. It generally needs to be approved by the requester's manager.[73] This authorisation step can be skipped to enable Users to directly submit requests for change.
- Phase 1, option 2: Request for change phase: in this phase, it is decided whether the request for change (RfC) will be processed as a simple change or an extensive change with multiple activities. Once a PRfC has been approved, the RfC needs to be approved by an Operator. Also, if the request has not already been linked to a premade change template, this can be done in this phase as well.

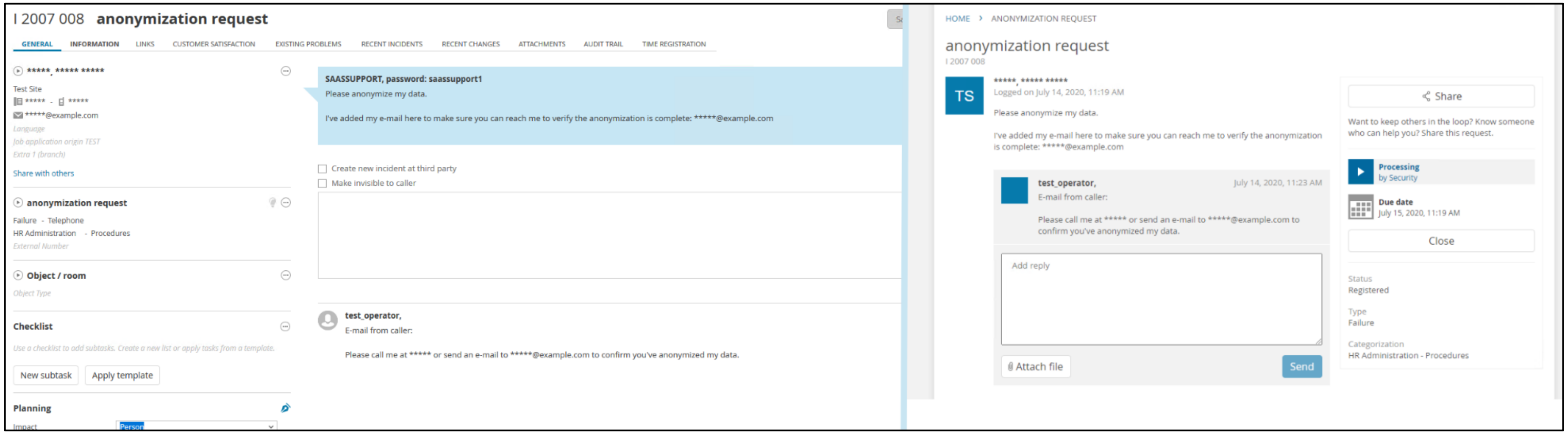
---

[73] If you have not selected a template, or the template does not specify who should authorise the PRfC, the requester's manager will be entered as the person who should submit the actual request.

- Phase 2: In progress phase: after authorisation, the simple change or first activity of the extensive change will appear in the applicable operator’s to-do list. When the deadlines of the change cannot be met, the planning can always be adjusted. Activities, or the change itself, can also be rejected at any time. This can be done via optional authorisation activities in the Self-Service Portal, for example.
- Phase 3: Evaluation phase (only for extensive changes): when an extensive change includes an evaluation phase, this phase is started after the ‘in progress phase’. This phase is mostly used for activities not directly required for the implementation of the change, such as setting up back-ups.[74]

Responsible data management: anonymisation

Screenshot 6: Example of an anonymisation request[75]



I 2007 008 **anonymization request**

*****, ***** *****
Test Site
***** - *****
*****@example.com
Language
Job application origin TEST
Extra 1 (branch)

anonymization request
Failure - Telephone
HR Administration - Procedures
External Number

Object / room
Object Type

Checklist
Use a checklist to add subtasks. Create a new list or apply tasks from a template.

Planning
Impact Person

SAASSUPPORT, password: saassupport1
Please anonymize my data.

I've added my e-mail here to make sure you can reach me to verify the anonymization is complete: *****@example.com

☐ Create new incident at third party
☐ Make invisible to caller

test_operator,
E-mail from caller:

Please call me at ***** or send an e-mail to *****@example.com to confirm you've anonymized my data.

anonymization request
I 2007 008

*****, ***** *****
Logged on July 14, 2020, 11:19 AM

Please anonymize my data.

I've added my e-mail here to make sure you can reach me to verify the anonymization is complete: *****@example.com

test_operator, July 14, 2020, 11:23 AM
E-mail from caller:

Please call me at ***** or send an e-mail to *****@example.com to confirm you've anonymized my data.

Want to keep others in the loop? Know someone who can help you? Share this request.

Processing
by Security

Due date
July 15, 2020, 11:19 AM

Status
Registered

Type
Failure

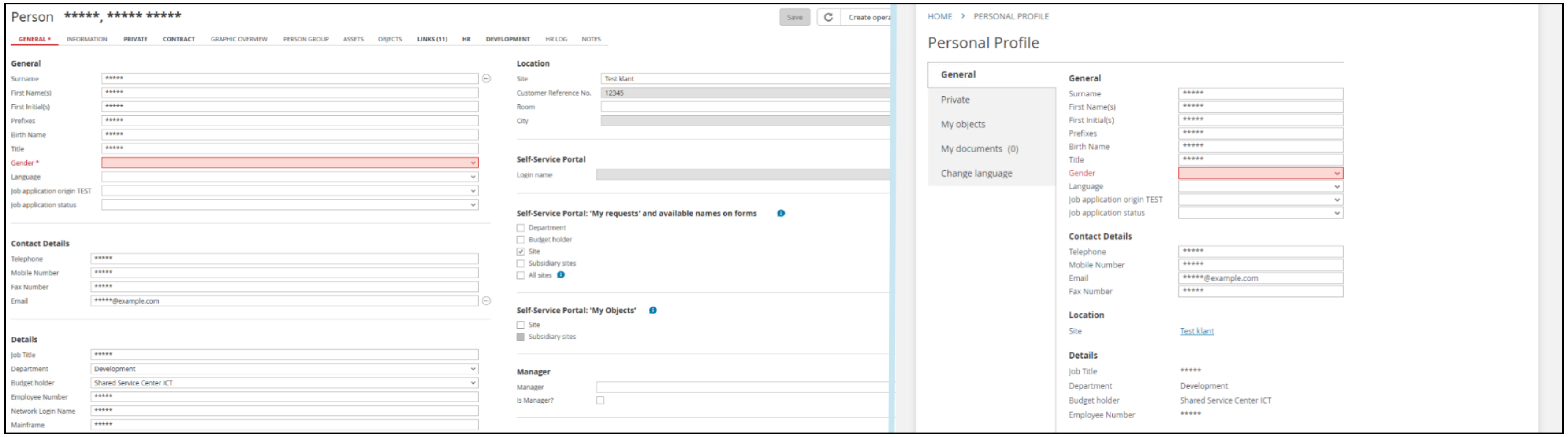
Categorization
HR Administration - Procedures

---

[74] https://docs.topdesk.com/en/change-management.html last accessed 25 April 2025.

[75] https://docs.topdesk.com/en/personal-data-protection.html last accessed 25 April 2025.

Screenshot 7: Example of the effect of a processed anonymisation request[76]



Person *****, ***** *****

General

Surname	*****
First Name(s)	*****
First Initial(s)	*****
Prefixes	*****
Birth Name	*****
Title	*****
Gender *	
Language	
Job application origin TEST	
Job application status	

Contact Details

Telephone	*****
Mobile Number	*****
Fax Number	*****
Email	*****@example.com

Details

Job Title	*****
Department	Development
Budget holder	Shared Service Center ICT
Employee Number	*****
Network Login Name	*****
Mainframe	*****

Location

Site	Test klant
Customer Reference No.	12345
Room	
City	

Self-Service Portal

Login name	

Self-Service Portal: 'My requests' and available names on forms

☐ Department
☐ Budget holder
☑ Site
☐ Subsidiary sites
☐ All sites

Self-Service Portal: 'My Objects'

☐ Site
▨ Subsidiary sites

Manager

Manager	
Is Manager?	☐

Personal Profile

General

Surname	*****
First Name(s)	*****
First Initial(s)	*****
Prefixes	*****
Birth Name	*****
Title	*****
Gender	
Language	
Job application origin TEST	
Job application status	

Contact Details

Telephone	*****
Mobile Number	*****
Email	*****@example.com
Fax Number	*****

Location

Site	Test klant

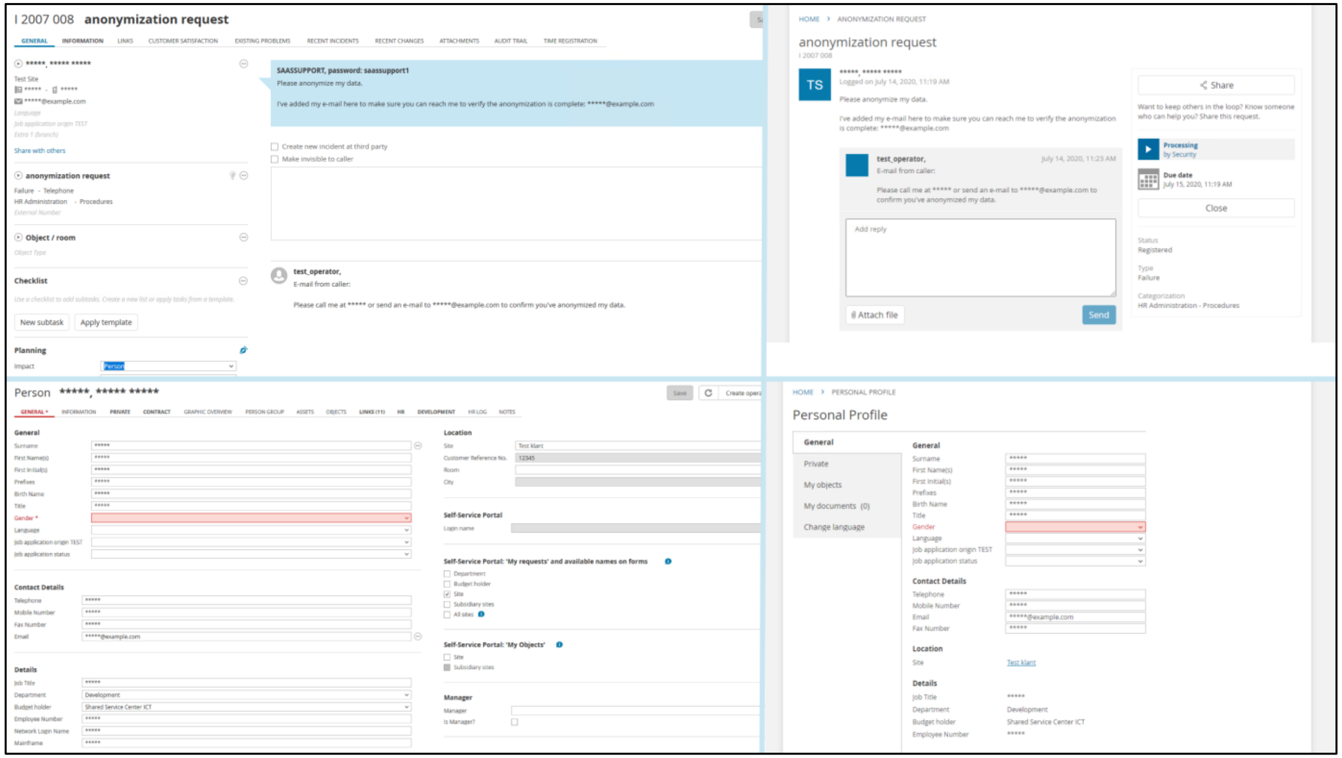
Details

Job Title	*****
Department	Development
Budget holder	Shared Service Center ICT
Employee Number	*****

---

[76] Ibid.

Screenshot 8: Example of the effect of a processed anonymisation request[77]



I 2007 008 **anonymization request**

*****, ***** *****
Test Site
***** · *****
*****@example.com
Language
Job application origin TEST
Extra 1 (branch)

anonymization request
Failure - Telephone
HR Administration - Procedures
External Number

Object / room
Object Type

Checklist
Use a checklist to add subtasks. Create a new list or apply tasks from a template.

Planning
Impact: Person

SAASSUPPORT, password: saassupport1
Please anonymize my data.

I've added my e-mail here to make sure you can reach me to verify the anonymization is complete: *****@example.com

☐ Create new incident at third party
☐ Make invisible to caller

test_operator,
E-mail from caller:

Please call me at ***** or send an e-mail to *****@example.com to confirm you've anonymized my data.

anonymization request
I 2007 008

TS *****, ***** *****
Logged on July 14, 2020, 11:19 AM
Please anonymize my data.

I've added my e-mail here to make sure you can reach me to verify the anonymization is complete: *****@example.com

test_operator, July 14, 2020, 11:23 AM
E-mail from caller:

Please call me at ***** or send an e-mail to *****@example.com to confirm you've anonymized my data.

Want to keep others in the loop? Know someone who can help you? Share this request.

Processing
by Security

Due date
July 15, 2020, 11:19 AM

Status
Registered

Type
Failure

Categorization
HR Administration - Procedures

Person *****, ***** *****

General
Surname: *****
First Name(s): *****
First Initial(s): *****
Prefixes: *****
Birth Name: *****
Title: *****
Gender *:
Language:
Job application origin TEST:
Job application status:

Contact Details
Telephone: *****
Mobile Number: *****
Fax Number: *****
Email: *****@example.com

Details
Job Title: *****
Department: Development
Budget holder: Shared Service Center ICT
Employee Number: *****
Network Login Name: *****
Mainframe: *****

Location
Site: Test klant
Customer Reference No.: 12345
Room:
City:

Self-Service Portal
Login name:

Self-Service Portal: 'My requests' and available names on forms
☐ Department
☐ Budget holder
☑ Site
☐ Subsidiary sites
☐ All sites

Self-Service Portal: 'My Objects'
☐ Site
☐ Subsidiary sites

Manager
Manager:
Is Manager? ☐

Personal Profile

General
Surname: *****
First Name(s): *****
First Initial(s): *****
Prefixes: *****
Birth Name: *****
Title: *****
Gender:
Language:
Job application origin TEST:
Job application status:

Contact Details
Telephone: *****
Mobile Number: *****
Email: *****@example.com
Fax Number: *****

Location
Site: Test klant

Details
Job Title: *****
Department: Development
Budget holder: Shared Service Center ICT
Employee Number: *****

---

[77] Ibid.

Annex 2: Overview security measures TOPdesk

- Separate DTAP environments
- A Security Information and Event Management (SIEM) system is used to detect attacks against our network in an early stage. These systems are monitored 24/7 by a Security Operations Centre with certified security experts.
- Institutions can use their own intrusion detection system and link this to the TOPdesk (access) logs. IP restrictions can be set up for institution’s TOPdesk SaaS environment, so only authorised Users have access to the TOPdesk environment.
- Antivirus and malware definitions are updated daily. File scans during upload, and regular full storage scans are performed.
- Data separation
    - An institution’s data is stored separate from other TOPdesk customers' data. Institution specific files (like attachments) are stored in a folder which can only be accessed by the institution’s dedicated TOPdesk environment. Folder and file permissions ensure that only the TOPdesk environment that created a file can access it.
    - A similar design is used for the database management; an institution’s TOPdesk environment can only connect to its dedicated database, and database permissions ensure that no application but the institution’s TOPdesk environment is allowed to access the data.

      This dual layer of security ensures that data remains segregated from other customers, and can never be accessed by unauthorized Users.
- Secure development: During development all software components and dependencies are scanned for known vulnerabilities. If no problems are found, the software is compiled and automatically tested. When all tests are successful, the software is deployed on a live environment which is scanned (black box) for vulnerabilities on a daily basis. A daily automated penetration test verifies if common or previously found issues can be exploited. These tests include known threats and OWASP vulnerabilities.

  The daily automated vulnerability scans and penetration tests are executed by an external auditor. To verify the scan results, improve future scans, and detect new issues specific to the TOPdesk software, a certified independent security expert performs a security test at least every 3 months.

  Institutions can also execute their own penetration tests or vulnerability scans after consulting with TOPdesk.
- Access management:
    - Access for Users: Many of the common identity providers (IdPs) can be linked to TOPdesk meaning an institution can control who has access to its TOPdesk environment, without setting up a separate login system. After linking TOPdesk to an existing IdP, Users can log in using Single sign-on (SSO) including all the institution’s security requirements like multi-factor authentication.
        - TOPdesk allows for role-based interfaces and authorizations, and access is adjustable on a granular level. Institutions can choose which services each User (or User group) has access to, and whether the User has read, write, or advanced

        permissions. Roles and permission groups can be defined and changed in the interface by selecting the appropriate permissions through checkboxes.

    - Access for TOPdesk: TOPdesk employees will only access an institution's TOPdesk SaaS environment, including Personal Data contained therein, when requested to do so, for instance when an institution's files a support ticket with TOPdesk. All TOPdesk Support staff that might be granted access have:
        - a certificate of conduct
        - a confidentiality agreement in their contract
        - completed an extensive training program regarding the TOPdesk products and hosting related topics such as handling confidential data and security awareness.
        - Institutions can also determine whether TOPdesk employees can access its TOPdesk environment and limit this to their geographical region. This can be configured through TOPdesk's Functional settings.
        - TOPdesk Support employees will only have access using a personal account from a secure TOPdesk authentication server.
        - Management access is limited to a small group of TOPdesk SaaS administrators and is only possible using a personal account and via a multi-factor authentication (MFA) gateway (see Access management). Separate servers are configured for management access, which are hardened and closely monitored.
        - TOPdesk employees take part in regular mandatory awareness, education and training activities in which attention is also had for (personal) data protection. Training progress is monitored and employees that do not complete their assigned trainings will have their access restricted automatically.
    - Access controls: Institutions can (automatically) download the access logs for their environment to verify who accessed the environment, and at what time. Access logs include all login attempts and information to identify the source, like IP addresses. As the access logs can be accessed automatically, they can be linked to an institution's own Intrusion Detection System.
        - Access logs are stored for half a year. If you'd like to store the logs for a longer period, you can download a copy.
        - Institutions can also request to make the full TOPdesk logs available for automated access. This allows the reviewing of all activity in the TOPdesk environment, including settings changes, permissions changes, and new accounts. The full TOPdesk logs will be available for up to 3 days, but a local copy can be stored for longer.

        It's possible to limit the availability of your TOPdesk environment to a certain IP range for additional security. To request an IP allow list, use the form on the My TOPdesk customer portal.

- Encryption
    - Encryption at rest: all Azure hosting locations use only encrypted disks for customer files, database back-ups and TOPdesk databases.
        - Data is distributed over multiple disk drives. This acts as a mitigatory measure in case of data loss, as a lost disk will only contain fragments of data.

  - Encryption in transit: A related risk to theft of stored data, is interception of data before it is stored. This risk is covered by only allowing encrypted connections (HTTPS) with TOPdesk SaaS environments. HSTS preloading ensures all connections are automatically started using HTTPS by all common browsers.

  - Regular checks determine whether there are Known Errors in used communication protocols, after which unsafe protocols are disabled as soon as possible. These measures resulted in an A+ score for the TOPdesk SaaS SSL certificate on Qualys SSL Labs, an independent party that assesses the strength of secure connections.[78]
- Data deletion: when deleting data from TOPdesk, this results in permanent irreversible deletion. The only options to recover deleted data, including data is:
  - Through an external back-up stored locally or with another 3rd party by the institution
  - By recovering an entire back-up, made by TOPdesk, from a specific time window. You cannot recover specific (fields on) Cards, Users or Operators – only the entire back-up from a specific time window can be restored. These back-ups are stored by TOPdesk for a period of 35 days.

In this regard, the configuration of authorisations is important, as only authorised Operators can delete data from TOPdesk. An alternative to data deletion, is archiving. TOPdesk contains an archiving function to remove – but not delete – data from the view of the majority of Users and Operators. Archived data can be restored by institution administrators that have the correct authorisations.

---

[78] https://page.topdesk.com/saas-information#servicesetupanddesign

Annex 3: Copy Data Subject Access Request

To: TOPdesk Privacy Team
TOPdesk B.V.
Westlandseweg 40
2624 AD Delft

6 August 2025

Subject: access to my Personal Data

Dear TOPdesk employee,

We have received a GDPR Access Request from the users listed below. This request is in accordance with Article 12 and Article 15, paragraph 1 of the General Data Protection Regulation (GDPR). We were able to handle a large part of the request ourselves, but there was a part of the request that were unable to handle ourselves. This concerns in particular the *“service log”* and the *“SaaS hosting server logs”*. However, the request covered *all the* data known about the applicants. Can you help us find the data that we do not have access to ourselves?

This concerns the data of the following users:

Name	**E-mailadres**	**Username**
Sanne Ouburg	sanne.ouburg@privacycompany.nl	SEOG
Arnold Roosendaal	arnold.roosendaal@privacycompany.nl	ADRL
Winfried Tilanus	winfried.tilanus@privacycompany.nl	WDTS
Evan Blommaert	evan.blommaert@privacycompany.nl	ENBT2

Over the period from 14-07-2025 to 16-07-2025.

During this period, these users connected from the IP addresses IPv4 85.238.129.232[79] and IPv6 2a10:3781:1fb::/32. These are fixed IP addresses for personal use.

These users contacted the environment: mboutrecht-test.topdesk.net.
We have established the identity of the users and have determined that the IP addresses mentioned are indeed in use by the users mentioned.

In addition, the users ask:

- For what purpose you have used the Personal Data of these Data Subjects.
- To which organisations or types of organisations you may have transferred the Personal Data of these Data Subjects.
- Whether you have transferred the Personal Data of these Data Subjects to a country outside the European Economic Area (EEA) or to an international organisation. And, if so, what measures you have taken to handle the Personal Data with care (appropriate safeguards for transfer).
- How long you retain the Personal Data of these Data Subjects.
- How you obtained the Personal Data of these Data Subjects, if they did not provide their data to you themselves.
- Whether you make automated decisions about people, including profiling. And if so, why you do so, on the basis of what logic and what consequences this may have for these Data Subjects.

Can you also look up this information?

In connection with the deadlines of the GDPR, I request that you look up this information within one month. If there are any problems in meeting this deadline or if the Processing unexpectedly takes longer, please let us know within two weeks so that we can fulfil our obligations.

When responding to this request, could you provide an overview of the files you searched and also mention any negative search results?
Many thanks and kind regards,

[NAME] & [NAME]

---

[79] This was the incorrect IP-address.

[NAME INSTITUTION]
[ADDRESS INSTITUTION]