Practical tips on how to use TOPdesk in a compliant way

1. Data scope and purpose

TOPdesk is an application that makes it easier to support your customers, whether they are colleagues or external customers of your organization. To offer effective support, it is often necessary to register some data like email address, phone numbers, an address and contact details regarding requests.

Depending on the type of services you provide and the type of relation with the data subject, it may vary what kind of information you need to register and how sensitive this data is. It helps to clearly document and communicate these details, so they can be used in the next steps. Using the TOPdesk Knowledge Base makes these details easily accessible to operators, and helps you to transparently communicate with your customers about how you handle their data.

2. Consent of data subject

In many situations TOPdesk is used to support employees and the organization's direct customers. As long as data registered in TOPdesk is necessary for the performance of a contract, like an employment or customer-supplier contract, to which the data subject is party, it is allowed to be processed without consent. However, if this is not clearly the case, explicit consent from the data subject is necessary.

3. Data access control

In line with the goal you have documented in the first step, certain people will have access to the information. In TOPdesk you are able to define permissions and filters to ensure only people have access that would actually need it. Linking TOPdesk to your central Identity system, like (Azure) Active Directory, will make sure that access to TOPdesk is always in line with your company security policies.

As working with data involves people, don't forget to instruct them on how to handle information before they gain access to it. A Security Awareness training is a good place to start. At TOPdesk we have examples of how to set up such trainings and our consultants are able to assist you with this.

4. Data retention policy

The GDPR mentions sensible retention policies. This means that you should think about how long it is necessary to have privacy sensitive data available, and make sure it is made untraceable after that time. The intention is to reduce the risk of unnecessarily exposing privacy sensitive data whenever a data leak should occur. For example, employees that have left the company 10 years ago, will still be affected by a leak that might happen today. That's why GDPR states that "old" data is to be removed (or made untraceable to an individual) in a timely fashion.

5. Selection of tools and suppliers

Carefully choosing which tools are used to register sensitive data is considered to be the responsibility of the controller. The chosen solution should enable the controller to take care of his responsibilities involved in properly handling personal data. If this is a cloud solution, this also includes the services delivered and involved management processes.

When selecting solutions and suppliers used to process personal data, don't forget to inform yourself about service setup and relevant auditing reports. Our ISAE 3000 audit report explains what kind of measures we have in place to provide a trustworthy service. You can contact your account manager to review this report.

6. Data Protection Agreements

When using SaaS software, make sure to have a Data Protection Agreement (DPA) in place. Such an agreement should contain clear explanations of the responsibilities of parties involved. This includes, for instance, a mutual confidentiality agreement, arrangements on how to work together in case of data breaches and how data is handled when ending the service contract. Make sure that sub-processors are included in the agreement chain. Of course, TOPdesk has taken care of contracts with any parties involved. We only use data centers that are able to deliver in line with our obligations towards our customers. And we have DPAs in place between our TOPdesk offices and the involved data centers.

Although there are quite a lot of generic templates going around for Data Protection Agreements, it is good to check with your supplier whether they have a specific DPA for their services. These are specifically written with the service delivered in mind and will save a lot of work.

7. Right to review, correct and "be forgotten"

Data subjects are helped by the GDPR to protect them from actions by others. GDPR gives them the right to review what has been registered about them. If needed, they can request that data is corrected or even deleted from your records.

It is good to inform your employees on how they should handle these requests if they come in. The Self-Service Portal is a way to provide transparency about what is registered. The knowledge base can be used to document what kind of data is registered and for what purpose. It is also used to show procedures so they are clear to both operators and customers.

Review of the data can be given on request, for instance using the print/export functionality in TOPdesk. Correction of erroneous data can be done directly in TOPdesk. For an individual, it is possible to overwrite personal data so that it is effectively no longer possible to identify that individual. This ensures the "right to be forgotten".

8. Set up a security incident process

Prevent stress when a data breach might occur, by setting up a security incident process now. This includes involving the correct expertise to assess the impact of an incident, identifying possibly needed actions to fix a leak and coordinate and execute (temporary) measures to resolve the situation.

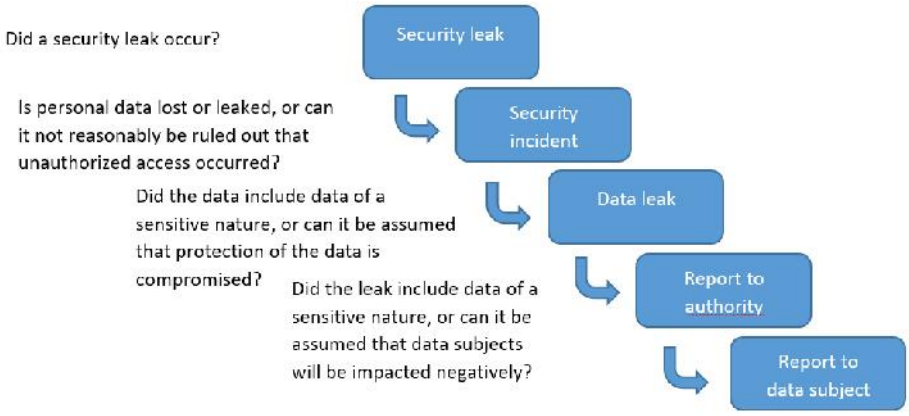
Having a security process in place, with named operators that will follow up, will help your organization to act as needed. Your TOPdesk consultant can also support you with that.

Consider a specific email address with TOPdesk mail import and a Self-Service Portal form that can be used to report security incidents. Using predefined categorization or operator groups, you can directly notify operators by email that a high priority incident is assigned to them.

The assigned operators will need to make some decisions when handling data leaks. In the best case, they will not often go through these procedures. Using forms and the knowledge base to document procedures will help your operators to follow up correctly. It also helps explain transparently to customers how you handle these situations.

9. Report data leaks

In some situations, you will have to report a security breach to the authorities and/or data subjects within 72 hours. But reporting too much or incorrectly might harm your organization's image. It is good practice to also include these procedures in your security incident process. And predetermine who will have the authority to decide on reporting leaks. The procedures might involve decision trees like these:



10. Have (adequate) security measures in place

Any application used to store sensitive data is subject to a set of measures. The application itself and underlying infrastructure, like operating systems, database servers, network etc., need to be securely configured and updated regularly to prevent known vulnerabilities from being used. When TOPdesk is used On Premises, both technical and procedural expertise is required to take care of this.

When using TOPdesk SaaS, you can depend on our organization's expertise to take care of this. Continuous Deployment, a service set up with security by design, a specialized team monitoring and maintaining the environments and regular security reviews by independent security experts help us make sure we stay on top of things. This unburdens you, so you can focus on your customer experience.

11. Report data leaks to the controller

If you use TOPdesk as a Service, and a data leak should occur, we have a security process in place to follow up on the leak. Incidents will be handled with the highest priority, making sure that you as controller are informed within 8 working hours after a leak becomes known. Actions will of course be taken to minimize impact and remediate any unwanted situation.

This will ensure that your company can follow up on your GDPR obligations and handle in line with your own security incident process.

12. Perform regular security tests and audits to check compliancy

We advise our customers to have their TOPdesk system (and any other systems holding sensitive data) validated periodically. No matter how good your own experts are, it is always possible that mistakes have been made. A default administrator password has not been reset, a reverse proxy running an outdated version etc. are easily overseen. This causes your valuable data to be at risk. Having security tests done by independent experts can help identify these vulnerabilities in time.

If you use TOPdesk SaaS, we take care of this for you. We also encourage our customers to have it checked again! We are very grateful for the many security reports we receive yearly. It complements the work of our own experts.

Pitfalls

Designing and documenting how you want to handle your data is doable in most cases. It is however easy to underestimate the time it takes to implement your choices. Especially instructing everyone involved and creating awareness of their own involvement can take some time.