E-BOOK

THE GDPR AND ITSM

TOP EIGHT ASPECTS OF ITSM MOST INFLUENCED BY THE GDPR

ManageEngine
ServiceDesk Plus

TABLE OF CONTENTS

The GDPR–
A brief overview

The GDPR–A brief overview

We can't talk about the General Data Protection Regulation (GDPR) without mentioning privacy. Privacy is the ability of an individual or group to seclude either themselves or information about themselves. Privacy is a fundamental right in most countries. But for a long time now, many organizations have taken privacy for granted, and the GDPR aims to change that by giving users control over how their personal data is used. The GDPR defines a set of rules and regulations to guide organizations around the world in dealing with the personal data of EU residents. Some of the major aspects of the GDPR are:

Key terms

Data subject

An identified or identifiable natural person.

Personal data

Any information relating to a data subject.

Personally identifiable information (PII)

An identified or identifiable natural person.

Data processing

Any operation or set of operations performed on personal data, such as collection, recording, storage, and deletion.

Scope of the GDPR

Affects any organization that processes EU residents' personal data.

Key players

Data controller

A person who decides how personal data is going to be processed.

Joint controller

Two or more people who decide how personal data is going to be processed.

Data processor

A person who processes data on behalf of the controller.

Recipients/sub-processor

A person who processes data for the processor.

Supervisory authorities

Independent authorities who monitor the application of the GDPR for a given state.

Key data *subject rights*

Key data subject rights

Data subject rights give individuals control over how their personal information is collected and processed by businesses. Some of the key data subject rights are:

- ### Transparency

  The details of data processing must be easily available in clear, plain language.

- ### Right of access

  Data subjects have the right to obtain information regarding what, why, and how their personal data is being processed.

- ### Right to rectification

  Data subjects have the right to obtain their personal data from the data controller and rectify any inaccuracies.

- ### Right to be forgotten

  Data subjects have the right to ask the controller to erase any personal data concerning them.

- ### Right to data portability

  Data subjects have the right to retrieve their personal data or transfer it to another controller.

- ### Right to restriction of processing

  Data subjects have the right to restrict the controller from processing their data based on personal situations, inaccurate data, unlawful processing, or if the data is no longer needed for processing.

- ### Right to object

  Data subjects have the right to object to the processing of their personal data at any point.

- ### Notification obligation

  The controller must notify the data subject in case there is a breach or if their personal data is being rectified or erased.

GDPR compliance:

It's everybody's job!

GDPR compliance: It's everybody's job!

According to a *survey* conducted by Deloitte earlier this year, only 15 percent of companies expected to be fully compliant with the GDPR by May 25, 2018. While May 25th has come and gone, organizations are re-evaluating their approach to privacy and how to build a model that is both operational and sustainable.

The first step is to recognize that it's no longer just the legal or privacy teams' jobs to achieve GDPR compliance. It's everybody's job. In most organizations, legal teams always have the last word when it comes to rules and regulations. Who can argue with their expertise? But, when it comes to the GDPR, those outside of these two departments can no longer use that same excuse. Every department in an organization falls under the purview of the GDPR if they deal with the personal data of EU residents.

Every department in an organization also deals with different sets of personal data and has its own processes and workflows, which makes it difficult to build a single compliance program that works throughout the entire organization. To summarize, these are some of the steps organizations should have taken (or should now take) to comply with the GDPR:

- Identify various collection points of personal data.
- Log all data processing activities.
- Review the data inventory and data flow across the organization.
- Have a consent mechanism in places where data is collected.
- Provide users with data access controls and have notifications in place for data infringement/leaks.
- Encrypt identified sensitive data at rest and in transit.
- Perform privacy risk assessments (both internally as well as by employing an external agency).
- Strengthen the privacy framework at the design level for products and services.

Keeping the above information in mind, let's explore how the GDPR impacts IT service desks, and how to build a GDPR compliance program for your IT service desk. But before we do that, it's important to understand the role of the IT service desk in the context of the GDPR. In general, most IT service desk teams deploy either an on-premises or cloud tool to run their operations. Based on the choice of deployment, your role as the IT service desk could vary. If you use:

On-premises tools, you could be both the ***data controller*** and the ***data processor.***

Cloud tools, you are the ***data controller*** while the cloud vendor is the ***data processor.***

Personal data
and IT service desks

Personal data and IT service desks

To understand the impact the GDPR has on IT service desks, we first have to look at how IT service desks deal with personal data. In this section, we'll discuss different types of personal data used by service desk teams and how this information is collected, processed, stored, and deleted.

Types of personal data

At first glance, it might seem that IT service desks mainly use personal data such as first names, last names, email addresses, and phone numbers, i.e. the data collected during request creation. But, when we take a closer look at the ITSM process, we realize that service desks are handling a lot more data than that. For example, when a user is provisioned a computer, their login ID, IP address, and MAC address is also shared as part of the process. These pieces of information are also considered PII since they're either unique to each user or can be used along with other personal data to identify a user. Now that we've identified the various types of personal data, it's time to look at how this data is processed.

Data collection

One way personal data enters a service desk is at the time of request creation, where basic information about the end user is collected for further communication and resolution. To illustrate that personal data can be collected at any stage of the ITSM process, let's consider a change request to update all Windows endpoint devices in an organization with the latest patch. To implement this change, the list of devices is obtained through various asset scanning techniques. To clearly see the different types of data in their systems, IT service desks must thoroughly analyze the various data collection points.

Data processing

Whether they're running reports for the monthly review meeting or analyzing the relationship between two different assets using the CMDB, IT service desks process data on a daily basis. Having a clear understanding of the various activities performed by the IT service desk helps with building data flow diagrams. For example, IP and MAC addresses are pulled when scanning IT assets. It's important to keep this in mind while mapping data flow in the service desk.

Storage and deletion

The GDPR requires organizations to take additional measures to protect the privacy of an individual, especially when storing their personal data. This means you need a tool that not only distinguishes personal data from other data, but also encrypts that personal data. In addition, the GDPR provides end users with the right to be forgotten. Upon request by the individual, the data controller (IT service desk teams) must be able to delete all the user's personal data in the system.

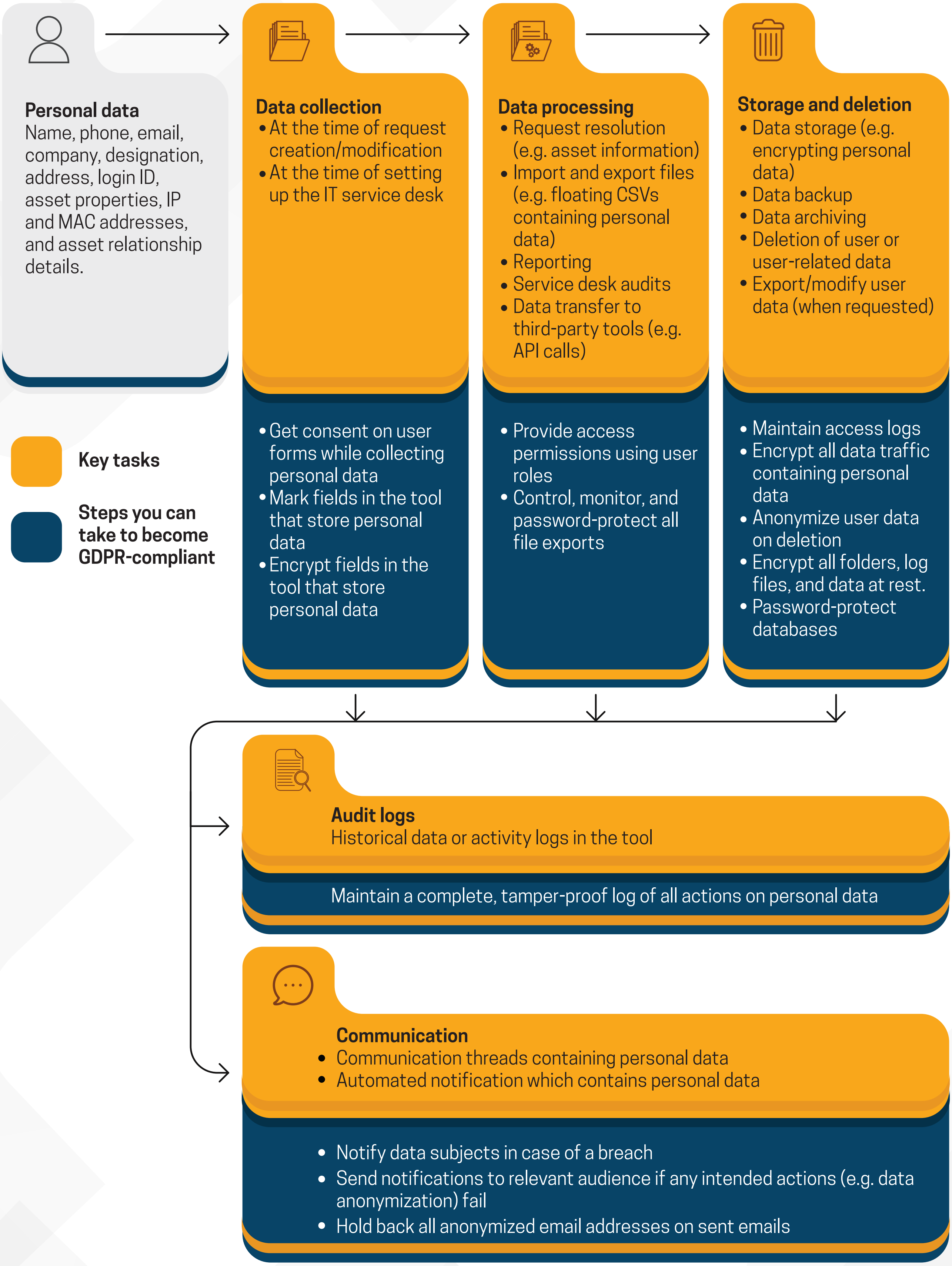
Communication

Most communication happens over email, phone, or chat. In most of these forms of communication, new conversation are attached to the older ones by default. Forwarding chains, for example, could lead to a potential leak of personal data to an unintended audience should that forwarded email leave your business' domain. This is why it's important to pay attention to the various forms of communication and how they work, which helps in tracing the flow of personal data in and out of the IT service desk.

Activity logs & audit trails

Most IT service desks collect historical data and log all activities for auditing purposes. While it may not seem like it, these activity logs might include personal data. For example, many technicians temporarily create a request in their name and later update the requestor details. Such updates get logged in the history of the request. It's often easy to miss these activities because personal data is not directly involved but is automatically logged by the system or tool.

Here's a visual representation of how personal data flows through a typical IT service desk:



Personal data
Name, phone, email, company, designation, address, login ID, asset properties, IP and MAC addresses, and asset relationship details.

🟧 **Key tasks**

🟦 **Steps you can take to become GDPR-compliant**

Data collection

- At the time of request creation/modification
- At the time of setting up the IT service desk

- Get consent on user forms while collecting personal data
- Mark fields in the tool that store personal data
- Encrypt fields in the tool that store personal data

Data processing

- Request resolution (e.g. asset information)
- Import and export files (e.g. floating CSVs containing personal data)
- Reporting
- Service desk audits
- Data transfer to third-party tools (e.g. API calls)

- Provide access permissions using user roles
- Control, monitor, and password-protect all file exports

Storage and deletion

- Data storage (e.g. encrypting personal data)
- Data backup
- Data archiving
- Deletion of user or user-related data
- Export/modify user data (when requested)

- Maintain access logs
- Encrypt all data traffic containing personal data
- Anonymize user data on deletion
- Encrypt all folders, log files, and data at rest.
- Password-protect databases

Audit logs
Historical data or activity logs in the tool

Maintain a complete, tamper-proof log of all actions on personal data

Communication

- Communication threads containing personal data
- Automated notification which contains personal data

- Notify data subjects in case of a breach
- Send notifications to relevant audience if any intended actions (e.g. data anonymization) fail
- Hold back all anonymized email addresses on sent emails

A brief note on *consent*

A brief note on consent

Other departments usually consult the IT service desk team before implementing any new tool. For example, IT service desk teams might be involved in establishing service management practices for HR, facilities, administrative staff, and other departments. This means IT service desks are responsible for ensuring that any tools they recommend have enough privacy controls to comply with various data protection regulations. With respect to the GDPR, this means recommending a tool that has a provision to request consent from end users.

Consent is one of the most important lawful bases for processing personal data and is used when you want to offer individuals control over how their data is being processed. This is particularly tricky because the GDPR has stricter rules for getting consent. For data subjects in the EU, the typical checkbox next to the terms of agreement no longer suffices.

The GDPR mandates that consent must be specific and granular. That is, the request for consent should clearly tell the user

a) how their data is going to be processed,
b) who will have access to that data,
c) whether or not any third-party controllers are involved, and
d) who the third-party controllers are and how those third parties will use the personal data.

In addition, the GDPR also requires:

- An explicit opt-in. Pre-ticked checkboxes or any other method of default consent aren't considered valid.
- End users be given an easy way to withdraw consent, including a clear explanation of how to go about doing that.
- A record of all evidence of consent.

What this means for IT service desks

When choosing an application to not only run your IT service desk but also assist other departments' help desks, it's a good idea to look for provisions within the application that allow you to get explicit consent from end users at the time of request logging.

For more information about consent visit,
https://gdpr-info.eu/art-7-gdpr/

How the GDPR *impacts ITSM*

How the GDPR impacts ITSM

The best way to understand how the GDPR affects IT service desks and ITSM processes is to look at some common scenarios and practices followed by IT service desk teams. By doing this, we can analyze privacy risks and see how teams can create privacy practices to protect the personal data of users.

User management

1. Bulk import of user data
2. Offboarding an employee

Asset management

3. Scanning for IT assets

Change management

4. Floating CSVs

Request management

5. Onboarding an employee

Notification and communication

6. Automated notifications

Reports

7. Export reports

Maintenance

8. Data archiving
9. Automated backup scheduling

Integrations

10. API calls

User management

User management is the most critical process when it comes to GDPR compliance, because it deals with managing users, creating user roles and groups, managing access privileges, and maintaining an accurate database of all users. Let's take a look at two scenarios to understand how the need for data protection impacts user management activities.

1. Bulk import of user data

When a new IT service desk tool is set up, the first task is to invite technicians and import users. Some methods used for importing user data are AD import, LDAP import, manul entry, or bulk import from CSV. Depending on the method used, the data being imported could vary. For example, AD import provides an option to import login name and domain name in addition to basic information such as name, designation, and department. Therefore, if you're using more than one of these methods for importing data, you need to know what kind of data it is as well as how that data is being imported. With so many ways to import user information, it can become tedious to trace where all this user information is being shared within the organization.

Things that could compromise data privacy

Multiple copies

Since each department uses and stores user data differently, organizations may find themselves with multiple copies of employee information in different formats, such as physical copies or online files.

Unaudited access

Access to user data might not be audited, especially if it's available as a physical copy or shared with group email addresses.

Ghost copies

Admins will often download a local copy of user data files to try and collate the user list. If they forget to delete this data after the import is completed, they'll end up with ghost copies of personal data.

Best practices to protect personal data

Identify personal data

Identify and map the types of personal data imported via different methods.

Configure access permissions

Provide access to decide who can view, modify, or delete user data.

Audit user access

Constantly monitor who is accessing the files that contain personal data.

Delete local copies

Make it a practice to delete local copies of files after the intended use.

2. Offboarding an employee

Many organizations have a set procedure for offboarding an employee, and it invariably involves keeping the IT service desk informed so that provisioned assets can be recovered, access to business applications can be revoked, and the user's account can be deleted. However with the GDPR, IT service desks now have additional responsibilities to protect data subjects' rights, such as the right to be forgotten and the right to data portability.

Whenever a user is deleted from the IT service desk, only their user account is deleted. This means there are still other places within the organization where the user may be referenced, like in ticket details pages or in past reports. The GDPR requires organizations to delete all instances of this information as well.

Things that could compromise data privacy

Email forwarding

Many organizations forward an ex-employee's emails to their manager's account for certain period of time after their exit.

Residual personal data

Employee information that was shared at different points in time might still be accessible from the system.

Access misuse

If their access isn't revoked in time, the offboarded employee could access the personal information of other employees or clients.

Single point of failure

If all of an employee's user credentials are deleted during the offboarding process, some of the apps they used may become inaccessible, preventing admins from deleting any PII stored in those applications.

Best practices to protect personal data

Identify all PII

Mark all the relevant personal data fields as PII so no PII is missed at the point of deletion.

Anonymize data

Anonymize the PII fields so that the related information can be used for processing even after the user data is deleted.

Revoke access

Revoke all system and application access that was provided to the user.

Replace login privileges

Ensure that there is a replacement for the deleted user's login privileges to avoid a single point of failure.

Enable data export

Provide a provision to export all user-related information when requested.

The GDPR & user management

Common PII used

Name, phone, email, company, designation, address, login credentials, and more.

Key data subject rights

Right to transparency, right to access, right to rectification, right to data portability, and notification obligation.

Best practices

- Identify and map personal data.
- Provide the right access permissions.
- Perform data cleanup regularly.
- Have provisions to anonymize data and export user data.

Asset management

The second most common time bulk data collection happens is during asset management. Asset management is the process of commissioning, maintaining, decommissioning, and taking inventory of IT assets. Sometimes that scope widens beyond IT assets as well. Since IT assets play a big role in request resolution, most tools available in the market either come with a built-in asset module or have tight integrations with third-party asset management software. IT asset information invariably includes IP addresses, which can be used to identify a person, meaning this process also comes under the purview of the GDPR.

3. Scanning for IT assets

Let’s use an employee request for a laptop as an example. To provision the laptop, the technician checks the availability of the required laptop and allocates accordingly. But before the technician can find this asset information, their organization’s IT assets need to be inventoried. You can do this through a Windows domain scan, network scan, or through a simple CSV import of asset data. Most of the time, these scans are scheduled at regular intervals to capture the current asset utilization. As these scans contain personal information, it’s important to know what measures need to be taken to keep data secure and private.

Things that could compromise data privacy

Unaudited access

Unaudited access to the asset inventory means that anyone can tamper with the asset information or gain illegal access to systems.

Prohibited software

Using prohibited software and devices could result in potential data leaks, including the personal data of users or clients.

Shared IT assets

Sometimes IT assets like a PC will be shared by two or more users and can lead to unwarranted access of data stored in the system.

Remote control and shadowing

Sysadmins are often given remote or shadow access to help resolve incidents. If this access isn't revoked after intended use, the end user's personal data may be at risk.

Asset leasing

When assets are leased to third parties, there's the risk that those third parties aren't taking proper security measures like data cleaning or configuring firewall access.

Best practices to protect personal data

Maintain asset history

Log each asset's ownership and access history.

Monitor shared assets

Ensure shared assets are regularly monitored and the correct permissions are provided for the shared drives.

Audit user permissions

Regularly audit user permissions to avoid misuse of temporary access.

Use software metering

Ensure that prohibited software is not used to fish information out of the organization network.

Configure roles for remote access

Create a dedicated role just for remote or shadow access, and map users to that role.

Set up security checks

Establish security and privacy procedures for leasing an asset to third parties.

The GDPR & asset management

Common PII used

Name, phone number, email, company, designation, address, asset properties, IP address, asset relationship details, MAC address, owner history, and login details.

Key data subject rights

Right to access, right to restriction of processing, and right to object.

Best practices

- Maintain asset history.
- Audit access.
- Revoke access after use.
- Establish security procedures for shared and leased assets.

Change management

Change management is all about minimizing risks while implementing IT changes. IT changes are usually either about updating an old system (e.g. patching or software upgrades) or about creating a new system (e.g. setting up a data center). Most of these changes follow a common workflow, which is change request submission, approval, planning, implementation, and review. Even though changes aren't directly involved in collecting or storing personal data, some changes involving IT assets could deal with asset information which might contain personal data.

3. Scanning for IT assets

Let's use upgrading servers from Windows Server 2012 to Windows Server 2016 as an example. The first thing that happens is a change plan is submitted to a committee consisting of stakeholders from various areas of the organization, also known as the change advisory board. This plan has the list of servers and applications, as well as the employees and clients that are accessing those applications. Based on the committee's recommendations, the plan can be modified and then scheduled for implementation.

The implementation is usually done over the weekend to minimize the impact of the change. During this process, the change record containing the personal information (available in the change and implementation document) gets circulated among various stakeholders. These floating documents could pose a serious threat to privacy if left unmonitored.

Things that could compromise data privacy

Forwarding chains

Stakeholders may share files containing personal data with their teams to keep them in the loop.

Notifications

Automated notifications could be sent to unintended recipients. This often happens when an employee changes departments and their email hasn't been taken off the notification list from their old department.

Local copies

Technicians may save a local copy of the change record or document for implementation and forget to delete it.

Historical data

The change history contains details of the change record, including the approver and technicians' details.

Best practices to protect personal data

Set up secure file sharing

Upload the change plans in file share software to monitor access history and provide permissions.

Clean up files

Make it a practice to clean up files regularly.

Leverage password protection

Add additional security, such as password protection, to any files that contain PII.

Configure notification roles

Use notification roles to avoid sending notifications to unintended recipients.

The GDPR & change management

Common PII used

IP address, asset allocation details, associated applications, and application access.

Key data subject rights

Right to access, right to restriction of processing, and right to object.

Best practices

- Use secure file sharing software.
- Clean up files regularly.
- Password-protect files whenever required.
- Use notification roles to avoid sending notifications to unintended recipients.

Request management

Request management is one of the IT service desk's major activities. Service desks are expected to maintain channels for raising requests, streamline ticketing to facilitate request fulfillment, and handle many other aspects of request management. IT service desks receive tickets about requests for information, asset provisioning, and even simple password resets. End users often don't provide enough information for the service desk to process their request, meaning the technician will need to reach out to the end user. For this purpose, some form of contact information–usually an email or phone number–is often collected during the time of request creation to facilitate further clarifications. Since this contact information is PII, IT service desk teams must take caution while handling this data.

5. Onboarding an employee

Many seasoned IT service desk teams use customizable templates for every type of request to collect all the required information. Teams often use additional fields to get the required information since most tools offer only a few basic fields by default. For example, while onboarding an employee, companies will collect personal data such as the employee's date of birth and residential address. This collected data is also shared with other departments such as HR to enroll the new employee in payroll, facilities to provide seating arrangements, and IT to provision assets.

Things that could compromise data privacy

Unclassified data

Without proper segregation between PII and unclassified data, it's hard to map and identify personal data, as well as provide additional security.

Common request templates

Sometimes users are asked to submit data that isn't relevant to their request.

Data sharing

When the request is passed on to a different team, all data is exposed instead of only the relevant data.

Best practices to protect personal data

Get consent

Ask for consent when collecting personal data.

Distinguish data

Have a provision to mark a field as PII.

Provide security

Have a provision to encrypt PII fields as needed.

Collect relevant data

Only collect information that is required.

Modify data

Have a provision to update personal data whenever there is a valid request.

Practice need-based sharing

When required, share only relevant information with other departments.

The GDPR & request management

Common PII used

Additional fields, resource fields, and allocation confirmation emails that contain PII.

Key data subject rights

Right to transparency, right to access, right to be forgotten, right to rectification, and notification obligation.

Best practices

- Request consent.
- Collect relevant data.
- Distinguish data.
- Encrypt data if required.
- Share only relevant information.

Notification and communication

IT service desk teams not only have internal teams based on skill level and expertise, but they also work with other departments within the company. This means there's a constant flow of information moving in and out of the IT service desk. Some of this information could be personal data, which is why it's important to analyze the role of the communication process in GDPR compliance.

6. Automated notifications

Automated notifications are triggered by actions, such as when a request is created or when a change is moved to the next stage of the change workflow. While these notifications certainly help in providing prompt resolution, they could also be a means through which personal data is shared with unintended recipients. Whenever a technician forwards request details to other teams (internally or to other departments) the request information containing personal data is also sent. While this often goes unnoticed, it's still considered a privacy risk.

Things that could compromise data privacy

Unintended recipients

If a technician is moved to a different department but left on their old department's notification list, they'll continue to have access to irrelevant PII.

Forwarding chains

With forwarding chains, PII might be shared even though it's not relevant to the recipient.

Best practices to protect personal data

Configure notification roles

Use roles to configure automated notifications.

Provide access links

Use a common link to provide access to the request instead of mentioning all the details in the notification email.

Conduct periodic audits

Regularly audit the automated notification settings to ensure only relevant people are informed.

Minimize email forwarding

Share the request details link instead of forwarding emails.

The GDPR & communications

Common PII used

Name, email, contact information, and IP address.

Key data subject rights

Right to access and right to notification obligation.

Best practices

- Configure notification roles.
- Provide access links to request information.
- Audit automatic notifications.

Reports

To measure the performance of the IT service desk and continually improve productivity, most IT service desks run periodic reports on service desk operations. These reports often contain personal data, but since this activity isn't a daily task, it can sometimes get overlooked when assessing the flow of personal data in the ITSM process.

7. Export reports

Reports are often exported for further analysis by the individual that ran the report or are shared within the IT service desk team or other teams in the organization. These reports are generally available as HTML, XLS, CSV, and PNG files. Be it a report on the number of requests served to a VIP user or a report on the number of SLA violations by technicians, these reports contain personal data, which means it's important to provide provisions for data protection.

Things that could compromise data privacy

Unchecked access

Downloaded reports could be shared with other teams within or outside the organization.

Local copies

Local copies of the reports are often created for analysis but are never deleted or archived.

Unlimited access

If technicians have unlimited access to run any type of query, they could expose personal data when it’s not required.

Best practices to protect personal data

Conduct a purpose check

Check the purpose of the report to see whether PII is required to analyze the report.

Set up security measures

Have a provision to password-protect files.

Configure access

Provide only a limited number of technicians with access to run query reports.

Delete outdated reports

Discard or archive reports after intended use.

Share access links

Use link shares instead of attachments.

Save activity logs

View version histories to know who changed what data.

The GDPR & reports

Common PII used

Requester details, technician information, and more.

Key data subject rights

Right to access and right to data portability.

Best practices

- Ensure that the PII is really required for analysis.
- Provide controlled access to run query reports.
- Use file sharing software instead of sending reports as attachments.

Maintenance

IT service desks perform a number of repetitive tasks while keeping track of the IT infrastructure's overall health. These maintenance activities might seem trivial when it comes to GDPR compliance, as most are automated and rarely require human intervention, but they can impact data security.

8. Data archiving

Many service desks archive data that isn't actively used in day-to-day operations to reduce their organization's storage consumption and manage costs. It's common practice for IT service desks to archive data related to closed requests, changes, and incidents dating back six or more months.

Things that could compromise data privacy

Unwarranted access

Unauthorized access to archived service desk data could lead to data misuse and manipulation.

Best practices to protect personal data

Leverage encryption

Encrypt archived data.

Enhance security

Password-protect archived files.

Configure roles

Create a permission mechanism to only allow certain users to schedule archiving.

9. Automated backup scheduling

IT service desks often schedule regular backups of their service desk data to facilitate quick restoration in case of any failures. Because of the amount of memory these backups take, they're often stored in a centralized location on the network drive.

Things that could compromise data privacy

Unmonitored access

The network drive could be shared with many other teams as well.

Best practices to protect personal data

Configure access permissions

Provide access privileges to both access old backups and schedule new ones.

Enhance security

Password-protect or encrypt backups.

The GDPR & maintenance

Common PII used

Requester details, technician information, and more.

Key data subject rights

Right to object and right to be forgotten.

Best practices

- Password-protect files.
- Encrypt data whenever required.
- Monitor access to all saved backups.

Integrations

IT service desk teams often work with many different departments to implement a change or fulfill a request. With a collaborative business environment, it's rare to find any application or tool that operates in silos. Most applications either have native integrations with other applications or have APIs to facilitate integrations. This means that personal data could be exposed to any third-party applications and therefore needs to be analyzed for GDPR compliance.

10. API calls

Not all tools provide native integrations to every application an organization uses. For example, IT service desk teams often schedule demo meetings with potential prospects using meeting applications like WebEx. To speed up the scheduling process, an IT service desk team might integrate their IT service desk tool with WebEx using an API. In this case, the prospect's name and email address, as well as the date and time of the meeting, are passed to WebEx using the API, and WebEx triggers a meeting invitation email to the provided email addresses. Even though APIs require authentication, personal data can still be misused since service desks don't have control over who can access the third-party application.

Things that could compromise data privacy

Unrestricted access

External applications might have unrestricted access to PII.

Best practices to protect personal data

Monitor access

Know what data is coming in and what is going out.

Document details

Keep updated documentation for every integration.

Maintain a repository

Keep a repository of all APIs.

Access logs

Automatically create logs for all the calls made to APIs.

The GDPR & integrations

Common PII used

Relevant PII such as name, contact information, and asset properties.

Key data subject rights

Right to transparency, right to restriction of processing, right to access, and right to object.

Best practices

- Monitor access.
- Keep updated documentation of all integrations.
- Maintain a repository of all APIs.
- Keep a log of all the calls made to APIs.

Summary

Summary

We've seen a few scenarios in ITSM which directly or indirectly deal with personal data, as well as what needs to be done to protect data privacy. Below is a summary of some of the common themes running across several modules of ITSM:

Data

Common activities that could compromise data privacy

- Using a common request template for all types of requests.
- Being unable to distinguish between PII and non-PII.
- Exposing data to other teams while processing a request.
- Sharing PII with third-party tools directly or via API.

Measures you can take to protect personal data

- Ask for consent when collecting personal data.
- Identify PII so you won't miss it during deletion.
- Collect only required information.
- Anonymize PII so that related information can still be used after a user is deleted.
- Have a provision to update personal data whenever there is a valid request.
- Share only relevant information with other departments and teams.

Files

Common activities that could compromise data privacy

- Having multiple copies of data circulating among different teams.
- Sharing files in forwarding email chains.
- Leaving local files unarchived or undisposed.

Measures you can take to protect personal data

- Use file sharing software to upload and update change plans, monitor access history, and provide permissions.
- Clean up files regularly.
- Password-protect any files that contain PII.
- Encrypt archived data.

Communication

Common activities that could compromise data privacy

- Forwarding email chains to share files among stakeholders and their teams.
- Sending automated notifications to unintended recipients.
- Forwarding requests to other teams via email.

Measures you can take to protect personal data

- Create roles for triggering notifications to avoid sending them to unintended recipients.
- Use a common link to provide access to a request instead of mentioning all the details in the notification email.
- Regularly audit the automated notification settings to ensure only relevant people are informed.

Communication

Common activities that could compromise data privacy

- Forwarding email chains to share files among stakeholders and their teams.
- Sending automated notifications to unintended recipients.
- Forwarding requests to other teams via email.

Measures you can take to protect personal data

- Create roles for triggering notifications to avoid sending them to unintended recipients.
- Use a common link to provide access to a request instead of mentioning all the details in the notification email.
- Regularly audit the automated notification settings to ensure only relevant people are informed.

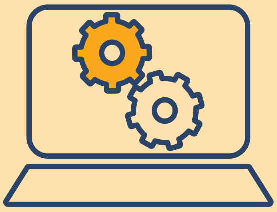
IT Ops

Common activities that could compromise data privacy

- Recording PII in activity logs within the tool.
- Leasing out assets without implementing security measures like data cleaning or firewall access.
- Neglecting to audit access to asset information.
- Forgetting to revoke remote control and shadowing access after intended use.
- Using prohibited software.
- Giving technicians unlimited access to run any type of query report.

Measures you can take to protect personal data

- When PII is deleted, make sure it's either anonymized or deleted from the history as well.
- Perform necessary security procedures whenever an asset is leased to third parties.
- Maintain a history of who has access to an asset and what actions were performed.
- Use roles for remote access and map users to these roles to keep control centralized.
- Use software metering to minimize the use of prohibited software.
- Allow a limited number of people to run query reports.
- Check the purpose of each report to see if PII is required for analysis. Use request and ticket IDs instead of PII.



Integrations

Common activities that could compromise data privacy

- Giving external applications unrestricted access to PII.

Measures you can take to protect personal data

- Know what data is coming in and what is going out.
- Keep documentation for every integration and update made.
- Keep a repository of all APIs.
- Automatically create logs for all the calls made to APIs.

Provisions in ServiceDesk Plus

to help you prepare for GDPR compliance

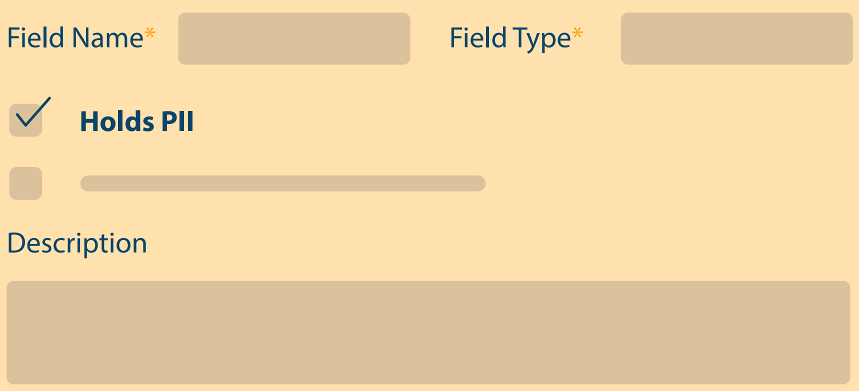
Provisions in ServiceDesk Plus to help you prepare for GDPR compliance

ServiceDesk Plus is ITIL®-ready help desk software used by over 100,000 IT service desks across 185 countries. It is a comprehensive ticketing tool with asset and project management capabilities. When it comes to GDPR compliance, ServiceDesk Plus provides several features to help you protect personal data.

Mark data fields as PII

Feature in ServiceDesk Plus

When adding an additional field to a template, you can easily distinguish PII from other data by marking that field as PII.



Field Name* Field Type*

☑ Holds PII

□

Description

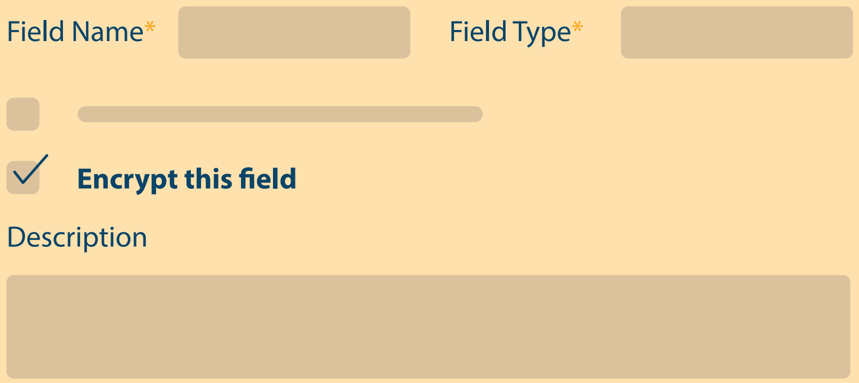
A few related GDPR Articles

Article 5 (1)(b) — Collect personal data only for specified purposes and do not process the data in any manner that is incompatible with the stated purpose(s).

Encrypt fields

Feature in ServiceDesk Plus

Encrypt sensitive information collected and stored from Request Additional Fields. Single line, multi-line, and pick list fields can all be encrypted.



Field Name* Field Type*

□

☑ **Encrypt this field**

Description

A few related GDPR Articles

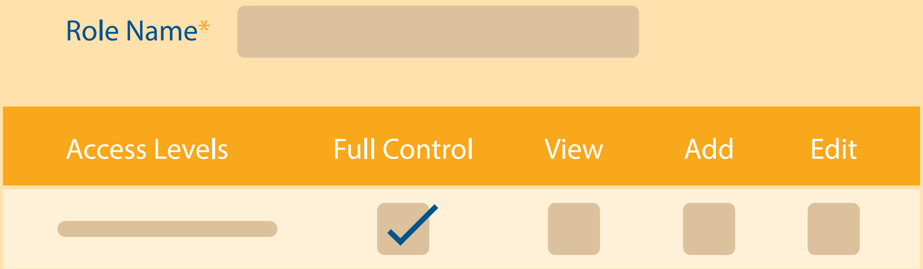
Article 5 (1)(f) — Process all forms of personal data with the utmost security and prevent unlawful or unauthorized means of processing.

Article 32(1)(a) — Ensure the confidentiality of all processing systems and encrypt personal data by implementing appropriate measures.

User roles

Feature in ServiceDesk Plus

Provide access permission to individual modules, as well as the activities that can be performed in those modules.



Role Name*

Access Levels	Full Control	View	Add	Edit
	☑	□	□	□

A few related GDPR Articles

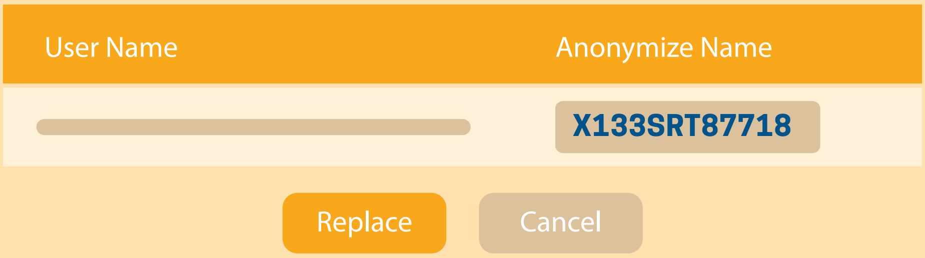
Article 25(2) — Personal data should be processed only for the purpose for which it was collected and should not be accessible to those who are not directly involved in these processes.

Article 32(4) — Take steps to ensure that nobody exploits or gains unauthorized or unlawful access to personal data.

Anonymize data

Feature in ServiceDesk Plus

Anonymize users' names and completely delete their other PII as needed.



User Name	Anonymize Name
	X133SRT87718

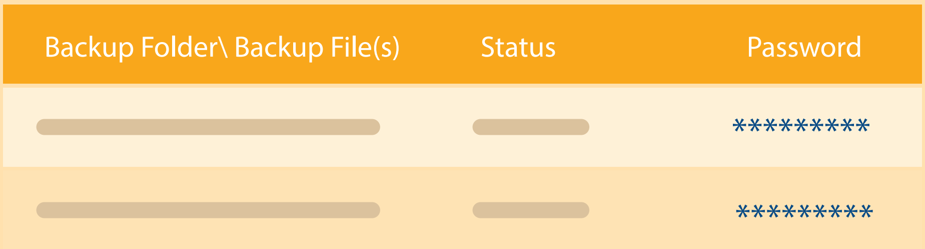
A few related GDPR Articles

Article 32 (1) (a) — Ensure the confidentiality of all processing systems and encrypt personal data by implementing appropriate measures.

Password protection

Feature in ServiceDesk Plus

Password-protect your backup files.



Backup Folder\ Backup File(s)	Status	Password
		*********
		*********

A few related GDPR Articles

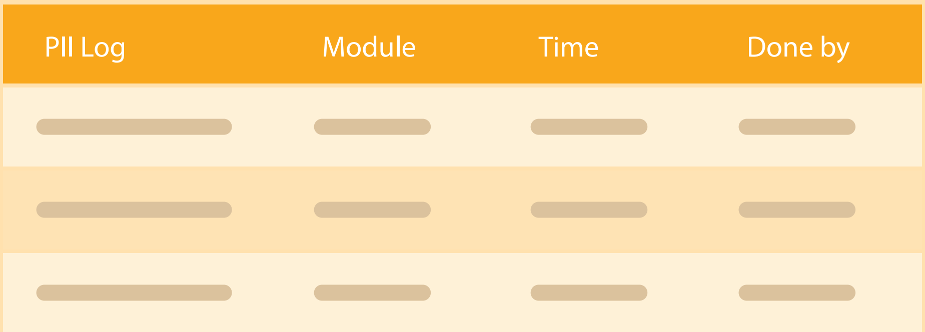
Article 32(4) — Take steps to ensure that nobody exploits or gains unauthorized or unlawful access to personal data.

Article 32(1)(a) — Ensure the confidentiality of all processing systems and encrypt personal data by implementing appropriate measures.

System logs and PII logs

Feature in ServiceDesk Plus

Log all activities performed in ServiceDesk Plus for auditing purposes.



PII Log	Module	Time	Done by

A few related GDPR Articles

Article 30 — Always maintain records of all processing activities with details about the reason for processing data, categories of data processed, and security measures undertaken during processing.

To learn more about these features in ServiceDesk Plus, visit https://www.manageengine.com/products/service-desk/gdpr-service-desk-software.html.

Conclusion

Conclusion

The GDPR is just the beginning of a wave of stricter privacy regulations. Many countries are waking up to the need for better data protection regulations, and businesses around the world are also starting to drive privacy initiatives across various functions. Since IT service desks are the bridge between IT and end users, they play a vital role in designing, developing, and communicating privacy measures. Implementing simple measures like those discussed could go a long way in creating a privacy culture in your organization.

Disclaimer: The information presented herein should not be used as legal advise. Please contact your legal advisor to learn how the GDPR impacts your specific organization and what you need to do to comply with the GDPR.

About ServiceDesk Plus

ServiceDesk Plus is ITIL-ready help desk software with integrated asset and project management capabilities. With advanced ITSM functionality and easy-to-use capability, ServiceDesk Plus helps IT support teams deliver world-class service to end users with reduced costs and complexity. It comes in three editions and is available in 29 different languages. Over 100,000 organizations across 185 countries trust ServiceDesk Plus to optimize IT service desk performance and achieve high end-user satisfaction.

To learn more about ServiceDesk Plus please visit www.manageengine.com/service-desk.

About ManageEngine

ManageEngine is bringing IT together for IT teams that need to deliver real-time services and support. Worldwide, established and emerging enterprises - including more than 60 percent of the Fortune 500 - rely on our real-time IT management tools to ensure tight business-IT alignment and optimal performance of their IT infrastructure, including networks, servers, applications, desktops and more. ManageEngine is a division of Zoho Corporation with offices worldwide, including the Netherlands, United States, India, Singapore, Japan and China.

For more information, please visit www.manageengine.com.