Data protection guide for operators

> **This guide is a working aid. It is not legal advice.**

As of 8 October 2026

You run the ticket system on your own server or VPS. For the personal data in your installation, your company is therefore the controller (EULA, section 9.1). This guide helps you use the ticket system in compliance with the GDPR.

Chapters A to C are templates. They contain a record of processing activities, the technical and organisational measures and a concept for retention and deletion. Chapter D shows how to handle requests from data subjects and data breaches in the product. Chapter E describes which data the installation sends to the manufacturer Smitey.

Names in quotation marks are labels on the screen. Check each statement against your own installation, as many points can be configured individually. Delete the rows for functions you do not use.

A. Record of processing activities

Art. 30 GDPR requires a record of processing activities. This template covers the ticket system. Fill in the four empty fields. Your other processing activities belong in your own record.

Field	Entry
Company	
Controller and contact details	
Data protection officer	
Hosting of the server	

Purposes and data

Purpose	Data subjects	Data
Handling requests	customers, external contacts, employees	name, e-mail address, phone number, ticket content, comments, attachments, ticket history
Managing user accounts	employees, customers with an account	name, e-mail address, sign-in name, department, position, location, role, team memberships, password as a hash, two-factor keys
Security log	users, administrators	failed sign-ins, account lockouts and password changes with IP address and browser; successful sign-ins only for administrators or after failed attempts; administrator actions with the name of the person acting
E-mail channel	senders and recipients of e-mails	e-mail address, subject, message text, attachments
Satisfaction survey	requesters of resolved tickets	e-mail address, rating, comment, proof of consent and unsubscribe
Time tracking	agents	name, booked time, note
Knowledge base	authors of articles	name, changes to articles

The satisfaction survey has two legal bases. External people receive it only after giving consent. The legal basis is consent under Art. 6(1)(a) GDPR. Your employees receive it without consent. The legal basis is a legitimate interest under Art. 6(1)(f) GDPR. Every survey e-mail contains a link to unsubscribe. With it, employees object and external people withdraw their consent. Under "Own e-mail domains" you set which addresses count as employees.

Data subjects

Employees with a staff account, such as agents and administrators. Customers with an account. External contacts without an account who are known only by their e-mail address.

Recipients

Employees of your company receive data according to their role and their teams. If you use the e-mail channel, your mail provider receives the e-mails. With single sign-on or a directory service, that

provider receives the sign-in data. Your hosting provider operates the server. Smitey receives no content of the installation. Chapter E lists the license data the installation sends.

Transfer to third countries

The software itself transfers no content to third countries. Whether a transfer takes place depends on your hosting provider, your mail provider and your sign-in provider.

Retention periods and measures

The retention periods are in chapter C. The technical and organisational measures are in chapter B.

B. Technical and organisational measures

Art. 32 GDPR requires appropriate technical and organisational measures. The first table lists what the software provides. The second table lists what you organise yourself. Add the measures of your company.

What the software provides

Measure	Implementation
Passwords	Passwords are stored only as a hash. You set length and character rules under "Password policy".
Failed sign-ins	By default, after 5 failed attempts for the same account, the system pauses the IP address they came from for 15 minutes. The account stays usable from other IP addresses. By default, after 20 failed attempts, the system locks the account itself for 15 minutes.
Two-factor authentication	Under "2FA Settings" you decide who needs an authenticator app at sign-in: "Off", "Administrators only", "Administrators and agents" or "Everyone". A new installation starts with "Administrators only". Anyone who has no second factor yet may postpone the setup at sign-in for at most 7 days. With single sign-on through an external provider, that provider handles the second factor.
Two-factor authentication in the profile	Every user can turn two-factor authentication on or off for their own account in the profile. Turning it on asks for the password and then for a code from the app. Turning it off asks for a current code. Turning it off is not possible while "2FA Settings" requires two-factor authentication for the user's role. Both are recorded in the "Security log".
Roles and permissions	Each role has its own permissions per function.
Teams	Agents work on the tickets of their teams.
Security log	Sign-in events and administrator actions are recorded under "Security log". Important events show a notice to everyone who may open the log. In the Professional edition they also send an e-mail.
Stored access data	Passwords for mailboxes and single sign-on are stored encrypted.
Encrypted backups	Backups are encrypted with AES-256. The key is stored protected on the server and additionally with the operator. This protects copies outside the server.
Updates	Update packages carry a signature. The installation checks it before it installs anything. Before an update, the system makes an encrypted backup. If this backup fails, the update changes nothing. If the database runs outside SMITEY, this backup does not contain it.
Browser protection	The included web server sends a content security policy. It limits which scripts a browser may run.
Encryption in transit	The installer sets up HTTPS in three ways: with your own certificate, with a certificate created by SMITEY for the local network, or with Let's Encrypt for a public domain. You switch later with "Change how SMITEY is reached". While an administrator works over plain HTTP, the system shows a notice.

Measure	Implementation
	From 30 days before your own certificate expires, administrators see a warning, from 7 days in red. In the Professional edition they also receive an e-mail. The HTTPS guide in the installation folder describes the steps.
Uploads	Attachments are only accepted for allowed file types and up to a size limit.
Retention periods	Old data is deleted or anonymized automatically. Chapter C lists the periods.
Data export	An administrator exports all data about a person as one file. Chapter D describes the steps.
Anonymization	Name and e-mail address of a person are replaced by a placeholder. Tickets and figures stay.

What you organise yourself

Measure	Your task
Server and hosting	Choose the server and the data centre. Keep the operating system up to date.
Encryption in transit	Turn on HTTPS for the installation. With a certificate created by SMITEY, install its root certificate on the computers that open the system. Renew your own certificate before it expires.
Backups	Make backups regularly. Decide how long you keep them. Store them protected from access by others. Keep the recovery key outside the server.
Access to the server	Allow only a few people to access the server and its files.
Updates	Install updates of the ticket system promptly.
User management	Give each person only the role they need. Delete the account when someone leaves.
Training	Instruct employees on data protection and on handling tickets.

C. Retention and deletion

The product deletes or anonymizes personal data after fixed periods. You change the periods under "Settings" → "Security" on the card "Data protection". Only the e-mail intake has its own setting under "E-Mail Settings".

Data	Default	Allowed	On by default
Sign-in events in the security log	90 days	7–365 days	yes
Administrator actions in the security log	12 months	1–120 months	yes
Deleted accounts	36 months	1–120 months	no
External contacts	36 months	1–120 months	no
Received e-mails	30 days	1 day or more	yes
Archive files	no period	–	–
Backups	set by you	–	–

Guiding rule: no period for tickets

Tickets have no retention period. Their content still serves a purpose, for example the customer history and business letters. A deletion by ticket age would also affect people who are still active. It would also change reports, deadlines and time tracking after the fact. Personal data is therefore anonymized when a person leaves or asks for deletion.

The individual periods

Sign-in events. The switch is "Delete old sign-in events", the field is "Days". Sign-in events contain IP address and browser. Old entries are deleted in the nightly run.

Administrator actions. The switch is "Delete old administrator actions", the field is "Months". Administrator actions show who changed what. The nightly run deletes old entries.

Deleted accounts. The switch is "Anonymize deleted users automatically". The period counts from the day the account was deleted. Name and e-mail address are replaced by a placeholder. Tickets and figures stay. When you switch it on, a preview shows who the first run will anonymize.

External contacts. The switch is "Anonymize external contacts automatically", the field is "Months without contact". It covers people without a staff account. The period counts from the last contact. People with an open ticket are skipped.

Received e-mails. The field is "Retention (days)". Messages older than this are deleted from the inbox and the processed folder. The system's own record of the received e-mails is deleted as well. The ticket created from an e-mail stays. This applies only if the e-mail intake is set up.

Archive files. Archive files have no period. You decide yourself when to delete an archive file. After someone is anonymized, the nightly run updates the archive files as well.

Backups. Backups are your responsibility. Write down in your concept for retention and deletion how long you keep them. By default, the backup program creates a backup every day. It keeps one backup each for the last 14 days, 4 weeks, 12 months, 4 quarters and 5 years. A backup can therefore be kept for about five years. It does not delete backups created by hand. You can change these numbers in the backup program. Set them in your concept for retention and deletion. These backups are in the folder "backups" of the installation folder. All new backups are encrypted. You find the recovery key in the file "SMITEY-credentials.txt" of the installation folder and in the backup program on the "Encryption" tab. Keep it outside the server. Without it, a backup cannot be read if the server is lost. If your database runs outside SMITEY, the backup program does not back it up.

Back it up with your own tools. Until the first update, or until you switch the backup program over by hand, the daily backup fails on such an installation. An anonymization does not change an existing backup. Anonymizations from before a restore are applied again. The card "Data protection" shows this under "Restore from a backup".

Backups before an update. Before every update, the product creates an encrypted backup through the backup program. It contains the database, the attachments and the archive files. If your database runs outside SMITEY, the backup contains only the attachments, the archive files and the keys, and the update still runs. Back up such a database with your own tools. The backup is in the backup folder like any other backup. The backup program keeps the 3 newest backups made before an update and deletes older ones. If the backup fails, the update changes nothing. The folder "Container" of the installation folder, subfolder "backups", now only holds the files needed to roll an update back. The update keeps the 3 newest folders there and deletes older ones itself. Backups from earlier versions (file extension .zip) are not encrypted. They stay readable and age out through the retention of the backup program. After the first new backup, the update deletes the copies of database, volumes and configuration file in old update folders.

The anonymizations run once a day at 03:00. The time zone is the one under "General Settings". Each block on the card shows the result of the last run in a line "Last run".

People who come back

A person may contact you again after an anonymization. Old anonymizations never affect their new data. When an anonymization is applied again, it only covers data that was created before it. This also applies after a backup or an archive has been restored.

Proof of anonymizations

"Download list of anonymizations" lists every anonymization so far. Keep this list. You need it if you restore an older backup.

D. Requests from data subjects and data breaches

This chapter shows the steps in the product for the main rights of data subjects. The procedure for a data breach comes at the end.

Deadline

Art. 12 GDPR requires an answer within one month. Note the date of receipt of each request.

Access

1. Open "User Management".
2. For a person with an account, click "Export personal data" in their row. For a person without an account, click "Export by e-mail address".
3. The dialog shows which data was found.
4. Click "Download". You receive a ZIP file. It contains one file per area in a machine-readable format and an overview for reading.
5. Check the export before you hand it over. Black out data of other people if needed.
6. Archived tickets are not included. Check your archives separately.

By default, only administrators may create the export. Each export is recorded.

Rectification

Correct the details of an account in "User Management". In the ticket itself you correct the requester details.

Erasure

Deleting and anonymizing are two different things. "Delete account" blocks sign-in and hides the account. "Restore account" brings it back. You fulfil a request for erasure with "Anonymize" in the same dialog as the export.

1. Open the dialog as described under Access.
2. Check retention duties first. Business letters, for example, must be kept for six years in Germany.
3. If needed, tick "Also clear the content of tickets this person requested".
4. Type ANONYMIZE and confirm.

Only an administrator can anonymize. This cannot be undone. Name and e-mail address are replaced by "Anonymized user" and a number.

The system can also anonymize deleted accounts and external contacts automatically after a period. Chapter C lists the switches and periods.

Objection

Some processing is based on a legitimate interest, for example the security log. A person may object to it. Check the objection in each case. The periods in chapter C limit the storage in any case.

Recipients of the satisfaction survey unsubscribe themselves with the link in each survey e-mail. If someone objects to you directly, record it under "Survey consents and unsubscribes" with "Record unsubscribe".

Data breaches

A data breach is a breach of security that leads to personal data being lost, altered or disclosed without authorization. Examples are a stolen backup, an account taken over by someone else or an e-mail sent to the wrong recipient. Backups are encrypted. If a backup was stolen, still check whether the recovery key may also have fallen into the wrong hands.

1. Stop the breach. Change passwords and deactivate affected accounts.
2. Find out what happened. The "Security log" shows failed attempts, account lockouts, the recorded sign-ins and administrator actions. You can filter it and export it.
3. Report the breach to the supervisory authority within 72 hours of becoming aware of it (Art. 33 GDPR). A report is not needed if the breach is unlikely to result in a risk to the persons concerned.
4. Inform the persons concerned if the risk to them is high (Art. 34 GDPR).
5. Document every breach, even one you do not report. Record the facts, the effects and the measures taken.

E. Data sent to the manufacturer

Purchased licenses are activated online and checked regularly with Smitey's license server. The demo sends a short report once a day. This chapter describes which data is sent and on which legal basis.

When the installation sends data

Activation. When you enter a purchased license key, the installation activates it. If no activation succeeds within 72 hours, the installation switches to a read-only mode. After the next successful check it works normally again.

Regular check. The installation contacts the license server every day. The first check runs shortly after every start of the installation. In three cases it tries every hour: while the license is not yet activated, while it is revoked and when the confirmation of the license has less than 72 hours left. If the checks fail for longer, the confirmation runs out. The installation then also switches to read-only mode. As soon as a check succeeds again, it works normally. If Smitey revokes a license, for example after a refund, the installation switches to read-only mode at the next check.

Offline keys. Smitey issues offline keys on request. An installation with an offline key also sends the data of the regular check every day, provided it reaches the license server. If it does not reach it, it still works normally.

Demo. Without a purchased license the demo sends a short report every day. The first report goes out shortly after every start of the installation.

On your click. Some buttons on the page "License" send data to the license server when you click them. "Contact license server now" sends the data of the regular check at once. In the demo it sends a demo report. "Redeem code" redeems an activation code from the purchase e-mail. "Request recovery license" requests a license for this installation after a reinstallation. "Deactivate license" releases the activation of this installation.

Update check. While someone who may install updates is signed in, the installation fetches the list of available updates from files.smitey.eu about every 30 minutes. It also downloads an update from there. This server of Smitey sees the IP address of the installation. The installation sends no other data in doing so.

What is sent

Occasion	Data
Activation	license ID, a random identifier of the installation, product version, operating system of the server
Regular check	the same data, plus the number of administrators, agents and teams
Demo	random identifier of the installation, remaining days of the demo, product version, operating system of the server
"Redeem code"	activation code, e-mail address from the purchase, random identifier of the installation
"Request recovery license"	license ID or e-mail address from the purchase, random identifier of the installation
"Deactivate license"	license ID, random identifier of the installation, product version
Update check	no data of the installation

The license server reads the IP address from the connection. From it, the server derives the approximate location, meaning country, region and city. The installation does not send either of them itself.

The installation sends no content. No tickets, no names of users, no e-mails and no attachments leave the installation. The e-mail address from the purchase is only sent when you redeem an activation code or recover a license. The demo report contains the e-mail address of the first administrator only if you chose this during installation.

Smitey deletes the IP address, region and city 12 months after the last contact. Only the country remains.

Legal basis

The online check is part of the license agreement. The legal basis is therefore the performance of the contract under Art. 6(1)(b) GDPR. As a fallback, Smitey relies on a legitimate interest under Art. 6(1)(f) GDPR. The balancing of interests:

Aspect	Assessment
Purpose	Detect misuse of licenses, such as one key used in several installations.
Data minimisation	Only the data in the table above. The e-mail address from the purchase is only sent on your click. No content, no names of users. The identifier of the installation is random.
Persons concerned	Licensees are mostly companies. The IP address is that of the company's server.
Transparency	The EULA, Smitey's privacy policy and this chapter describe the transfer.
Period	IP address, region and city are deleted 12 months after the last contact.

No switch for purchased licenses

The check of purchased licenses cannot be switched off. It is part of the license.

The daily demo report can be switched off at any time. On Windows, run the setup again and clear the box "Send the daily demo report". On Linux, run the installation script again and answer "Switch off the daily demo report? (yes/no)" with yes. The setting is stored as DEMO_REPORT in the configuration file of the installation. The button "Contact license server now" still sends a single demo report when you click it.

No data processing agreement

Smitey processes no data on your behalf. The installation sends no content of the installation to Smitey. A data processing agreement is therefore not required (EULA, section 9.3).