

Datenschutz-Leitfaden für Betreiber

Dieser Leitfaden ist eine Arbeitshilfe. Er ist keine Rechtsberatung.

Stand: 6. Oktober 2026

Sie betreiben das Ticket-System auf Ihrem eigenen Server oder VPS. Für die personenbezogenen Daten in Ihrer Installation ist deshalb Ihre Firma der Verantwortliche (EULA, Ziffer 9.1). Dieser Leitfaden hilft bei der Umsetzung, das Ticket-System DSGVO-konform zu nutzen.

Die Kapitel A bis C sind Vorlagen. Sie enthalten ein Verzeichnis von Verarbeitungstätigkeiten, die technischen und organisatorischen Maßnahmen und ein Löschkonzept. Kapitel D zeigt, wie Sie Anfragen betroffener Personen und Datenpannen im Produkt bearbeiten. Kapitel E beschreibt, welche Daten die Installation an den Hersteller Smitey sendet.

Namen in Anführungszeichen sind Beschriftungen auf dem Bildschirm. Prüfen Sie jede Aussage gegen Ihre eigene Installation, da viele Punkte individuell konfigurierbar sind. Streichen Sie die Zeilen für Funktionen, die Sie nicht nutzen.

A. Verzeichnis von Verarbeitungstätigkeiten

Art. 30 DSGVO verlangt ein Verzeichnis von Verarbeitungstätigkeiten. Diese Vorlage deckt das Ticket-System ab. Füllen Sie die vier leeren Felder aus. Ihre übrigen Verarbeitungen gehören in Ihr eigenes Verzeichnis.

Feld	Eintrag
Firma	
Verantwortlicher und Kontaktdaten	
Datenschutzbeauftragter	
Hosting des Servers	

Zwecke und Daten

Zweck	Betroffene	Daten
Bearbeitung von Anfragen	Kunden, externe Kontakte, Mitarbeiter	Name, E-Mail-Adresse, Telefonnummer, Ticketinhalt, Kommentare, Anhänge, Ticketverlauf
Verwaltung der Benutzerkonten	Mitarbeiter, Kunden mit Konto	Name, E-Mail-Adresse, Anmeldename, Abteilung, Position, Standort, Rolle, Teamzugehörigkeiten, Passwort als Hash, Schlüssel der Zwei-Faktor-Anmeldung
Sicherheitsprotokoll	Benutzer, Administratoren	fehlgeschlagene Anmeldungen, Kontosperrungen und Passwortänderungen mit IP-Adresse und Browser; erfolgreiche Anmeldungen nur bei Administratoren oder nach Fehlversuchen; Verwaltungsaktionen mit dem Namen der handelnden Person
E-Mail-Kanal	Absender und Empfänger von E-Mails	E-Mail-Adresse, Betreff, Nachrichtentext, Anhänge
Zufriedenheitsumfrage	Anfragende gelöster Tickets	E-Mail-Adresse, Bewertung, Kommentar
Zeiterfassung	Agenten	Name, gebuchte Zeit, Notiz
Wissensdatenbank	Autoren von Artikeln	Name, Änderungen an Artikeln

Betroffene

Mitarbeiter mit einem Mitarbeiterkonto, zum Beispiel Agenten und Administratoren. Kunden mit einem Konto. Externe Kontakte ohne Konto, die nur über ihre E-Mail-Adresse bekannt sind.

Empfänger

Die Mitarbeiter Ihrer Firma erhalten Daten nach ihrer Rolle und ihren Teams. Nutzen Sie den E-Mail-Kanal, erhält Ihr Mailanbieter die E-Mails. Bei Single Sign-On oder einem Verzeichnisdienst erhält dieser Anbieter die Anmeldedaten. Ihr Hosting-Anbieter betreibt den Server. Smithey erhält keine Inhalte der Installation. Kapitel E nennt die Lizenzdaten, die die Installation sendet.

Übermittlung in Drittländer

Die Software selbst übermittelt keine Inhalte in Drittländer. Ob eine Übermittlung stattfindet, hängt von Ihrem Hosting-Anbieter, Ihrem Mailanbieter und Ihrem Anmeldedienst ab.

Fristen und Maßnahmen

Die Fristen stehen in Kapitel C. Die technischen und organisatorischen Maßnahmen stehen in Kapitel B.

B. Technische und organisatorische Maßnahmen

Art. 32 DSGVO verlangt geeignete technische und organisatorische Maßnahmen. Die erste Tabelle nennt, was die Software mitbringt. Die zweite Tabelle nennt, was Sie selbst regeln. Ergänzen Sie die Maßnahmen Ihrer Firma.

Was die Software mitbringt

Maßnahme	Umsetzung
Passwörter	Passwörter werden nur als Hash gespeichert. Regeln für Länge und Zeichen legen Sie unter „Password policy“ fest.
Fehlgeschlagene Anmeldungen	Als Werkseinstellung pausiert das System nach 5 Fehlversuchen für dasselbe Konto die IP-Adresse, von der sie kamen, für 15 Minuten. Von anderen IP-Adressen bleibt das Konto nutzbar. Nach 20 Fehlversuchen sperrt das System als Werkseinstellung das Konto selbst für 15 Minuten.
Zwei-Faktor-Anmeldung	Unter „2FA Settings“ verlangen Sie bei der Anmeldung eine Authenticator-App. Sie wählen zwischen nur Mitarbeitern und allen Benutzern.
Rollen und Rechte	Jede Rolle hat eigene Rechte je Funktion.
Teams	Agenten arbeiten an den Tickets ihrer Teams.
Sicherheitsprotokoll	Anmeldeereignisse und Verwaltungsaktionen stehen im „Security log“. Wichtige Ereignisse zeigen allen, die das Protokoll öffnen dürfen, einen Hinweis. In der Professional-Edition verschicken sie zusätzlich eine E-Mail.
Gespeicherte Zugangsdaten	Passwörter für Postfächer und Single Sign-On werden verschlüsselt gespeichert.
Updates	Update-Pakete tragen eine Signatur. Die Installation prüft sie, bevor sie etwas installiert. Vor einem Update legt das System eine vollständige Sicherung an.
Schutz im Browser	Der mitgelieferte Webserver sendet eine Content Security Policy. Sie begrenzt, welche Skripte ein Browser ausführen darf.
Uploads	Anhänge werden nur für erlaubte Dateitypen und bis zu einer Größengrenze angenommen.
Fristen	Alte Daten werden automatisch gelöscht oder anonymisiert. Kapitel C nennt die Fristen.
Datenauskunft	Ein Administrator exportiert alle Daten zu einer Person als eine Datei. Kapitel D beschreibt die Schritte.
Anonymisierung	Name und E-Mail-Adresse einer Person werden durch einen Platzhalter ersetzt. Tickets und Kennzahlen bleiben.

Was Sie selbst regeln

Maßnahme	Ihre Aufgabe
Server und Hosting	Wählen Sie Server und Rechenzentrum. Halten Sie das Betriebssystem aktuell.

Maßnahme	Ihre Aufgabe
Verschlüsselung der Verbindung	Schalten Sie HTTPS für die Installation ein.
Sicherungen	Legen Sie regelmäßig Sicherungen an. Legen Sie fest, wie lange Sie sie aufbewahren. Bewahren Sie sie vor fremdem Zugriff geschützt auf.
Zugang zum Server	Geben Sie nur wenigen Personen Zugang zum Server und seinen Dateien.
Updates	Spielen Sie Updates des Ticket-Systems zeitnah ein.
Benutzerverwaltung	Geben Sie jeder Person nur die Rolle, die sie braucht. Löschen Sie das Konto, wenn jemand ausscheidet.
Schulung	Weisen Sie die Mitarbeiter in den Datenschutz und den Umgang mit Tickets ein.

C. Löschkonzept

Das Produkt löscht oder anonymisiert personenbezogene Daten nach festen Fristen. Die Fristen ändern Sie unter „Settings“ → „Security“ auf der Karte „Data protection“. Nur der E-Mail-Eingang hat eine eigene Einstellung unter „E-Mail Settings“.

Daten	Werkseinstellung	Erlaubt	Werkseitig an
Anmeldeereignisse im Sicherheitsprotokoll	90 Tage	7–365 Tage	ja
Verwaltungsaktionen im Sicherheitsprotokoll	12 Monate	1–120 Monate	ja
Gelöschte Konten	36 Monate	1–120 Monate	nein
Externe Kontakte	36 Monate	1–120 Monate	nein
Eingegangene E-Mails	30 Tage	1 Tag oder mehr	ja
Archivdateien	keine Frist	–	–
Sicherungen	legen Sie fest	–	–

Leitregel: keine Frist für Tickets

Tickets haben keine Aufbewahrungsfrist. Ihr Inhalt erfüllt weiter einen Zweck, zum Beispiel die Kundenhistorie und Geschäftsbriefe. Eine Löschung nach dem Alter des Tickets träfe auch Personen, die noch aktiv sind. Sie würde außerdem Berichte, Fristen und Zeiterfassung nachträglich verändern. Personenbezogene Daten werden deshalb anonymisiert, wenn eine Person ausscheidet oder die Löschung verlangt.

Die einzelnen Fristen

Anmeldeereignisse. Der Schalter heißt „Delete old sign-in events“, das Feld „Days“.

Anmeldeereignisse enthalten IP-Adresse und Browser. Alte Einträge werden im Nachlauf gelöscht.

Verwaltungsaktionen. Der Schalter heißt „Delete old administrator actions“, das Feld „Months“.

Verwaltungsaktionen zeigen, wer was geändert hat. Der Nachlauf löscht alte Einträge.

Gelöschte Konten. Der Schalter heißt „Anonymize deleted users automatically“. Die Frist zählt ab dem Tag, an dem das Konto gelöscht wurde. Name und E-Mail-Adresse werden durch einen Platzhalter ersetzt. Tickets und Kennzahlen bleiben. Beim Einschalten zeigt eine Vorschau, wen der erste Lauf anonymisiert.

Externe Kontakte. Der Schalter heißt „Anonymize external contacts automatically“, das Feld „Months without contact“. Es betrifft Personen ohne Mitarbeiterkonto. Die Frist zählt ab dem letzten Kontakt. Personen mit einem offenen Ticket werden übersprungen.

Eingegangene E-Mails. Das Feld heißt „Retention (days)“. Ältere Nachrichten werden aus dem Posteingang und dem Ordner für verarbeitete Nachrichten gelöscht. Auch die Aufzeichnung des Systems über die eingegangenen E-Mails wird gelöscht. Das Ticket, das aus einer E-Mail entstanden ist, bleibt. Das gilt nur, wenn der E-Mail-Eingang eingerichtet ist.

Archivdateien. Archivdateien haben keine Frist. Wann Sie eine Archivdatei löschen, entscheiden Sie selbst. Nach einer Anonymisierung schreibt der Nachlauf auch die Archivdateien neu.

Sicherungen. Für Sicherungen sind Sie selbst zuständig. Halten Sie in Ihrem Löschkonzept fest, wie lange Sie sie aufbewahren. Als Werkseinstellung legt das Sicherungsprogramm jeden Tag eine Sicherung an. Es bewahrt je eine Sicherung der letzten 14 Tage, 4 Wochen, 12 Monate, 4 Quartale und 5 Jahre auf. Eine Sicherung kann damit rund fünf Jahre alt werden. Von Hand angelegte Sicherungen löscht es nicht. Diese Zahlen können Sie im Sicherungsprogramm ändern. Legen Sie sie in Ihrem Löschkonzept fest. Diese Sicherungen liegen im Ordner „backups“ des Installationsordners. Eine Anonymisierung ändert keine vorhandene Sicherung. Anonymisierungen aus der Zeit vor einer Wiederherstellung werden erneut angewendet. Die Karte „Data protection“ zeigt das unter „Restore from a backup“.

Sicherungen vor einem Update. Vor jedem Update legt das Produkt eine vollständige Sicherung an. Sie enthält die Datenbank, die Anhänge und die Archivdateien. Sie liegt im Ordner „Container“ des Installationsordners im Unterordner „backups“. Unter Linux ist das als Werkseinstellung der Ordner /opt/smitey/Container/backups. Das Produkt löscht diese Sicherungen nie selbst. Legen Sie fest, wie lange Sie sie aufbewahren, und löschen Sie ältere Sicherungen selbst.

Die Anonymisierungen laufen einmal am Tag um 03:00 Uhr. Es gilt die Zeitzone unter „General Settings“. Jeder Block der Karte zeigt das Ergebnis des letzten Laufs in einer Zeile „Last run“.

Personen, die zurückkommen

Eine Person kann sich nach einer Anonymisierung wieder melden. Alte Anonymisierungen treffen ihre neuen Daten nie. Wird eine Anonymisierung erneut angewendet, erfasst sie nur Daten, die vor ihr entstanden sind. Das gilt auch, nachdem eine Sicherung oder ein Archiv zurückgespielt wurde.

Nachweis der Anonymisierungen

„Download list of anonymizations“ listet jede bisherige Anonymisierung auf. Bewahren Sie diese Liste auf. Sie brauchen sie, wenn Sie eine ältere Sicherung einspielen.

D. Anfragen betroffener Personen und Datenpannen

Dieses Kapitel zeigt die Schritte im Produkt für die wichtigsten Rechte betroffener Personen. Am Ende steht das Vorgehen bei einer Datenpanne.

Frist

Art. 12 DSGVO verlangt eine Antwort innerhalb eines Monats. Notieren Sie das Eingangsdatum jeder Anfrage.

Auskunft

1. Öffnen Sie „User Management“.
2. Klicken Sie bei einer Person mit Konto in ihrer Zeile auf „Export personal data“. Bei einer Person ohne Konto klicken Sie auf „Export by e-mail address“.
3. Der Dialog zeigt, welche Daten gefunden wurden.
4. Klicken Sie auf „Download“. Sie erhalten eine ZIP-Datei. Sie enthält je Bereich eine maschinenlesbare Datei und eine Übersicht zum Lesen.
5. Prüfen Sie den Export, bevor Sie ihn weitergeben. Schwärzen Sie bei Bedarf Daten anderer Personen.
6. Archivierte Tickets sind nicht enthalten. Prüfen Sie Ihre Archive getrennt.

Als Werkseinstellung dürfen nur Administratoren den Export anlegen. Jeder Export wird aufgezeichnet.

Berichtigung

Die Angaben eines Kontos berichtigen Sie in „User Management“. Im Ticket selbst berichtigen Sie die Angaben zum Anfragenden.

Löschung

Löschen und Anonymisieren sind zwei verschiedene Dinge. „Delete account“ sperrt die Anmeldung und blendet das Konto aus. „Restore account“ holt es zurück. Einen Löschantrag erfüllen Sie mit „Anonymize“ im selben Dialog wie den Export.

1. Öffnen Sie den Dialog wie unter Auskunft beschrieben.
2. Prüfen Sie zuerst Aufbewahrungspflichten. Geschäftsbriefe müssen in Deutschland zum Beispiel sechs Jahre aufbewahrt werden.
3. Setzen Sie bei Bedarf den Haken „Also clear the content of tickets this person requested“.
4. Tippen Sie ANONYMIZE ein und bestätigen Sie.

Anonymisieren kann nur ein Administrator. Das lässt sich nicht rückgängig machen. Name und E-Mail-Adresse werden durch „Anonymized user“ und eine Nummer ersetzt.

Gelöschte Konten und externe Kontakte kann das System nach einer Frist auch automatisch anonymisieren. Kapitel C nennt die Schalter und Fristen.

Widerspruch

Manche Verarbeitungen beruhen auf einem berechtigten Interesse, zum Beispiel das Sicherheitsprotokoll. Eine Person kann ihnen widersprechen. Prüfen Sie den Widerspruch im Einzelfall. Die Fristen aus Kapitel C begrenzen die Speicherung in jedem Fall.

Datenpannen

Eine Datenpanne ist eine Verletzung der Sicherheit, durch die personenbezogene Daten verloren gehen, verändert werden oder unbefugt offengelegt werden. Beispiele sind eine gestohlene Sicherung, ein von Fremden übernommenes Konto oder eine E-Mail an den falschen Empfänger.

1. Stoppen Sie die Panne. Ändern Sie Passwörter und deaktivieren Sie betroffene Konten.
2. Klären Sie, was geschehen ist. Das „Security log“ zeigt Fehlversuche, Kontosperrungen, die aufgezeichneten Anmeldungen und Verwaltungsaktionen. Sie können es filtern und exportieren.
3. Melden Sie die Panne innerhalb von 72 Stunden der Aufsichtsbehörde, nachdem sie Ihnen bekannt wurde (Art. 33 DSGVO). Eine Meldung entfällt, wenn die Panne voraussichtlich kein Risiko für die betroffenen Personen bringt.
4. Benachrichtigen Sie die betroffenen Personen, wenn das Risiko für sie hoch ist (Art. 34 DSGVO).
5. Dokumentieren Sie jede Panne, auch eine, die Sie nicht melden. Halten Sie Sachverhalt, Auswirkungen und ergriffene Maßnahmen fest.

E. Datenübermittlung an den Hersteller

Gekaufte Lizenzen werden online aktiviert und regelmäßig beim Lizenzserver von Smitey geprüft. Die Demo sendet einmal am Tag eine kurze Meldung. Dieses Kapitel beschreibt, welche Daten dabei übertragen werden und auf welcher Rechtsgrundlage.

Wann die Installation Daten sendet

Aktivierung. Wenn Sie einen gekauften Lizenzschlüssel eingeben, aktiviert die Installation ihn. Gelingt innerhalb von 72 Stunden keine Aktivierung, wechselt die Installation in einen Nur-Lese-Modus. Nach der nächsten erfolgreichen Prüfung arbeitet sie wieder normal.

Regelmäßige Prüfung. Die Installation meldet sich jeden Tag beim Lizenzserver. Die erste Prüfung läuft kurz nach jedem Start der Installation. In drei Fällen versucht sie es stündlich: solange die Lizenz noch nicht aktiviert ist, solange sie widerrufen ist und wenn die Bestätigung der Lizenz weniger als 72 Stunden Restlaufzeit hat. Scheitern die Prüfungen länger, läuft die Bestätigung ab. Die Installation wechselt dann ebenfalls in den Nur-Lese-Modus. Sobald eine Prüfung wieder gelingt, arbeitet sie normal. Widerruft Smitey eine Lizenz, zum Beispiel nach einer Erstattung, wechselt die Installation bei der nächsten Prüfung in den Nur-Lese-Modus.

Offline-Schlüssel. Smitey stellt Offline-Schlüssel auf Anfrage aus. Auch eine Installation mit Offline-Schlüssel sendet jeden Tag die Daten der regelmäßigen Prüfung, sofern sie den Lizenzserver erreicht. Erreicht sie ihn nicht, arbeitet sie trotzdem normal.

Demo. Ohne gekaufte Lizenz sendet die Demo jeden Tag eine kurze Meldung. Die erste Meldung geht kurz nach jedem Start der Installation hinaus.

Auf Ihren Klick. Einige Schaltflächen auf der Seite „License“ senden Daten an den Lizenzserver, wenn Sie sie anklicken. „Contact license server now“ sendet sofort die Daten der regelmäßigen Prüfung. In der Demo sendet sie eine Meldung der Demo. „Redeem code“ löst einen Aktivierungscode aus der Kauf-E-Mail ein. „Request recovery license“ fordert nach einer Neuinstallation eine Lizenz für diese Installation an. „Deactivate license“ gibt die Aktivierung dieser Installation frei.

Suche nach Updates. Solange jemand angemeldet ist, der Updates einspielen darf, ruft die Installation etwa alle 30 Minuten die Liste der verfügbaren Updates von files.smitey.eu ab. Auch ein Update lädt sie von dort. Dabei sieht dieser Server von Smitey die IP-Adresse der Installation. Weitere Daten sendet die Installation dabei nicht.

Was übertragen wird

Anlass	Daten
Aktivierung	Lizenz-ID, eine zufällige Kennung der Installation, Produktversion, Betriebssystem des Servers
Regelmäßige Prüfung	dieselben Daten, dazu die Zahl der Administratoren, Agenten und Teams
Demo	zufällige Kennung der Installation, Resttage der Demo, Produktversion, Betriebssystem des Servers
„Redeem code“	Aktivierungscode, E-Mail-Adresse aus dem Kauf, zufällige Kennung der Installation
„Request recovery license“	Lizenz-ID oder E-Mail-Adresse aus dem Kauf, zufällige Kennung der Installation

Anlass	Daten
„Deactivate license“	Lizenz-ID, zufällige Kennung der Installation, Produktversion
Suche nach Updates	keine Daten der Installation

Der Lizenzserver liest die IP-Adresse aus der Verbindung. Aus ihr leitet er den ungefähren Standort ab, also Land, Region und Ort. Beides sendet die Installation nicht selbst.

Die Installation sendet keine Inhalte. Keine Tickets, keine Namen von Benutzern, keine E-Mails und keine Anhänge verlassen die Installation. Die E-Mail-Adresse aus dem Kauf geht nur mit, wenn Sie einen Aktivierungscode einlösen oder eine Lizenz wiederherstellen. Die Meldung der Demo enthält die E-Mail-Adresse des ersten Administrators nur, wenn Sie das bei der Installation gewählt haben.

Smitey löscht IP-Adresse, Region und Ort 12 Monate nach dem letzten Kontakt. Nur das Land bleibt.

Rechtsgrundlage

Die Online-Prüfung ist Teil des Lizenzvertrags. Rechtsgrundlage ist deshalb die Erfüllung des Vertrags nach Art. 6 Abs. 1 lit. b DSGVO. Hilfsweise stützt sich Smitey auf ein berechtigtes Interesse nach Art. 6 Abs. 1 lit. f DSGVO. Die Abwägung:

Gesichtspunkt	Bewertung
Zweck	Missbrauch von Lizenzen erkennen, zum Beispiel einen Schlüssel in mehreren Installationen.
Datensparsamkeit	Nur die Daten aus der Tabelle oben. Die E-Mail-Adresse aus dem Kauf geht nur auf Ihren Klick mit. Keine Inhalte, keine Namen von Benutzern. Die Kennung der Installation ist zufällig.
Betroffene	Lizenznehmer sind meist Firmen. Die IP-Adresse ist die des Servers der Firma.
Transparenz	Die EULA, die Datenschutzerklärung von Smitey und dieses Kapitel beschreiben die Übermittlung.
Frist	IP-Adresse, Region und Ort werden 12 Monate nach dem letzten Kontakt gelöscht.

Kein Schalter für gekaufte Lizenzen

Die Prüfung gekaufter Lizenzen lässt sich nicht abschalten. Sie ist Teil der Lizenz.

Die tägliche Meldung der Demo können Sie jederzeit abschalten. Unter Windows führen Sie das Setup erneut aus und entfernen den Haken „Tägliche Demo-Meldung senden“. Unter Linux führen Sie das Installationsskript erneut aus und beantworten „Tägliche Demo-Meldung abschalten? (ja/nein)“ mit ja. Die Einstellung steht als DEMO_REPORT in der Konfigurationsdatei der Installation. Die Schaltfläche „Contact license server now“ sendet auf Ihren Klick trotzdem eine einzelne Meldung der Demo.

Kein Auftragsverarbeitungsvertrag

Smitey verarbeitet keine Daten in Ihrem Auftrag. Die Installation sendet keine Inhalte an Smitey. Ein Auftragsverarbeitungsvertrag ist deshalb nicht nötig (EULA, Ziffer 9.3).