> **Archived version 1.0, valid from February 11, 2026 to October 31, 2026.**
>
> Current version: https://helpdesk.portali.space/legal/privacy

Privacy Policy

Version: 1.0 · Valid from February 11, 2026 to October 31, 2026

Last updated: February 11, 2026

---

1. Data Controller

The controller of personal data is:

TTN, s.r.o.
Sadová 2719/3A, 905 01 Senica, Slovak Republic
Company ID (IČO): 52330443 | Tax ID (DIČ): 2120984085 | VAT ID: SK2120984085
E-mail: privacy@ttn.sk

(hereinafter "Controller" or "we")

This Privacy Policy (hereinafter "Policy") explains how we collect, process, store and protect personal data of users of the WLP customer portal (hereinafter "Portal").

The Portal is operated under the brands WorkSys.Space, FacilityUp.Space, CitySys.Space and TTN. Regardless of the brand used, the Controller is always TTN, s.r.o.

---

2. Personal Data We Collect

2.1. Data Provided by the User

Category	Examples	Purpose
Identification data	Name, surname, e-mail address	Registration, authentication, communication
Organizational data	Organization name, job title	Organization assignment, SLA management
Ticket content	Subject, problem description, comments, attachments	Providing customer support
Communication data	E-mail correspondence, notifications	Informing about ticket status

2.2. Data Collected Automatically

Category	Examples	Purpose
Technical data	IP address, browser type, operating system	Security, diagnostics
Usage data	Access logs, clicks, time spent on pages	Service improvement
Cookies	Sessions, language preferences	Portal functionality

2.3. Data from the AI Assistant (if activated)

Category	Examples	Purpose
User questions	Text of questions entered into the AI chat	Generating responses
AI context	Relevant ticket numbers, KB articles (anonymized)	Contextual responses
AI responses	Text of generated responses	Display to the User
AI metadata	Token count, response time, model used	Monitoring, billing

---

3. Purposes and Legal Bases for Processing

3.1. Overview of Purposes

Purpose	Legal Basis (GDPR)	Retention
Providing Services (helpdesk, KB, reporting)	Performance of contract — Art. 6(1)(b)	Duration of account + 3 years
Account management and authentication	Performance of contract — Art. 6(1)(b)	Duration of account
E-mail notifications about tickets	Performance of contract — Art. 6(1)(b)	Duration of account
AI Assistant — generating responses	Consent — Art. 6(1)(a)	Locally: duration of account. At Anthropic: max. 7 days
Security and abuse prevention	Legitimate interest — Art. 6(1)(f)	12 months
Service improvement (anonymous analytics)	Legitimate interest — Art. 6(1)(f)	24 months (anonymized)
Legal compliance	Legal obligation — Art. 6(1)(c)	As required by applicable law

3.2. Legitimate Interests

Where the legal basis is legitimate interest (Art. 6(1)(f)), this relates to:
- ensuring the security and integrity of the Portal,
- fraud and abuse prevention,
- improving the quality of Services based on anonymized analytics.

These interests have been assessed through a balancing test and do not override the rights and freedoms of data subjects.

---

4. Recipients of Personal Data

4.1. Categories of Recipients

Recipient	Purpose	Location	Safeguards
Anthropic PBC	Processing AI Assistant queries	USA	DPA + Standard Contractual Clauses (SCC)
Mailgun (Sinch)	Delivering e-mail notifications	EU/USA	DPA + SCC
Hosting provider (Laravel Forge / DigitalOcean)	Portal infrastructure hosting	EU	DPA, ISO 27001
Organization administrators	Managing users within their organization	—	Contractual terms

4.2. Transfers to Third Countries

Personal data are transferred to the USA (Anthropic PBC, potentially Mailgun). These transfers are secured by:
- **Standard Contractual Clauses (SCC)** pursuant to European Commission Decision 2021/914,
- **Data Processing Addendum (DPA)** with the respective processors,
- additional supplementary measures where applicable (encryption, data minimization).

---

5. Cookies and Similar Technologies

5.1. Strictly Necessary Cookies

The Portal uses strictly necessary (functional) cookies to ensure basic functionality:

Cookie	Purpose	Duration
session	User login and session	Until browser is closed
XSRF-TOKEN	CSRF attack protection	2 hours
locale	Language preferences	1 year
dark_mode	Dark mode preference	1 year
ai_consent	AI Assistant consent storage	1 year

These cookies are strictly necessary for Portal operation and do not require consent under Art. 5(3) of Directive 2002/58/EC (ePrivacy).

5.2. Analytics Cookies

The Portal currently does not use third-party analytics cookies (Google Analytics, Facebook Pixel, etc.). If this changes in the future, the User will be asked for consent through a cookie banner.

---

6. AI Assistant — Data Processing

6.1. Description of Processing

The AI Assistant is an optional Portal feature that uses the **Claude API** service from **Anthropic PBC** (San Francisco, USA) to automatically answer Users' questions.

When a User asks a question to the AI Assistant:
1. The User's question is sent to the Operator's server.
2. The server assembles context (relevant KB articles, ticket status) and **anonymizes personal data** before sending.
3. The anonymized question with context is sent to the Anthropic API.
4. The Anthropic API returns a generated response.
5. The response is de-anonymized and displayed to the User.

6.2. Anonymization

Before sending data to the Anthropic API, anonymization is performed:
- names of persons are replaced with generic labels (e.g. "Customer", "Agent"),
- e-mail addresses are replaced with placeholder text "[email]",
- phone numbers, IP addresses, company IDs and other identifiers are removed or replaced.

The aim is to minimize the scope of personal data transferred to the third party.

6.3. Anthropic API Safeguards

Property	Detail
Training on data	Anthropic **never** uses API data to train its models
Data retention	Anthropic retains API logs for a maximum of **7 days**, then automatically deleted
Contractual basis	Data Processing Addendum (DPA) with Standard Contractual Clauses (SCC)
Zero-Data-Retention	Zero retention mode is available for enterprise customers
Role of Anthropic	Processor within the meaning of Art. 4(8) GDPR
Certifications	SOC 2 Type II

More information: https://privacy.claude.com

6.4. Legal Basis

Processing of data through the AI Assistant is based on the **User's consent** (Art. 6(1)(a) GDPR). Consent is requested before first use of the AI Assistant and may be withdrawn at any time.

6.5. Consequences of Consent Withdrawal

Withdrawal of consent:
- disables the AI Assistant for the given User,
- does not affect the lawfulness of processing prior to withdrawal,
- does not affect other Portal Services.

6.6. Local Storage of AI Conversations

AI conversations (questions and responses) are stored in the Controller's database for the purposes of:
- continuing the conversation,
- improving response quality,
- audit logging for security purposes.

The User may request deletion of their AI history at any time (see Art. 8).

---

7. Data Retention Periods

Data Category	Retention Period
Account data (name, e-mail)	Duration of account + 3 years after deletion
Ticket content	Duration of account + 3 years after deletion

Data Category	Retention Period
E-mail notifications	12 months
AI conversations (local)	Duration of account (User may delete at any time)
AI data at Anthropic	Max. 7 days (automatic deletion)
Security logs	12 months
Invoices and accounting documents	10 years (legal obligation)

After the retention period expires, data are securely deleted or anonymized.

---

8. Data Subject Rights

Under Regulation (EU) 2016/679 (GDPR), you have the following rights:

8.1. Right of Access (Art. 15)

You have the right to obtain confirmation as to whether your personal data are being processed, and if so, to access them and information about the processing.

8.2. Right to Rectification (Art. 16)

You have the right to have inaccurate personal data corrected and incomplete data supplemented.

8.3. Right to Erasure (Art. 17)

You have the right to request erasure of your personal data if:
- the data are no longer necessary for the purposes for which they were collected,
- you withdraw consent (e.g. for the AI Assistant) and there is no other legal basis,
- you object to processing and there are no overriding legitimate grounds.

For AI history: Users can delete AI conversations directly in the Portal settings.

8.4. Right to Restriction of Processing (Art. 18)

You have the right to request restriction of processing in cases specified by the GDPR.

8.5. Right to Data Portability (Art. 20)

You have the right to receive your personal data in a structured, commonly used and machine-readable format (JSON) and to transmit them to another controller.

8.6. Right to Object (Art. 21)

You have the right to object to processing based on legitimate interest. In such case, we will cease processing unless we demonstrate compelling legitimate grounds.

8.7. Right to Withdraw Consent (Art. 7(3))

Where processing is based on consent (e.g. AI Assistant), you have the right to withdraw consent at any time. Withdrawal does not affect the lawfulness of processing prior to withdrawal.

8.8. Right to Lodge a Complaint

You have the right to lodge a complaint with the supervisory authority:

Office for Personal Data Protection of the Slovak Republic
Galvaniho Business Centrum II, Galvaniho 7/B, 821 04 Bratislava, Slovakia
Web: https://dataprotection.gov.sk
E-mail: statny.dozor@pdp.gov.sk
Phone: +421 2 32 31 32 14, +421 2 32 31 32 49

8.9. Exercising Your Rights

You may exercise your rights:
- By e-mail to: **privacy@ttn.sk**

- In writing to the Controller's registered office

We will respond to your request **within 30 days** of receipt. In justified cases, this period may be extended by a further 2 months, of which we will inform you.

---

9. Data Security

9.1. The Controller implements appropriate technical and organizational measures to protect personal data, including:

Measure	Detail
Encryption in transit	TLS 1.2+ (HTTPS) on all endpoints
Encryption at rest	Database and backup encryption
Access control	Role-based access control (RBAC) — Users see only data they are authorized to access
Brand isolation	Data are strictly separated between brands — a customer of one brand never sees data of another
Data minimization	Anonymization of personal data before sending to external APIs
Audit log	Records of access, changes and AI interactions
Backup	Regular encrypted backups
ISO 27001	The Controller is ISO 27001 certified
Incident response	Defined procedure for security incidents including notification to the supervisory authority within 72 hours pursuant to Art. 33 GDPR

---

10. Changes to This Policy

10.1. The Controller reserves the right to update this Policy, particularly due to legislative changes, addition of new Services or changes in data processing.

10.2. Users will be informed of material changes through:
- a notice on the Portal,
- an e-mail notification.

10.3. The date of the last update is always indicated at the beginning of this document.

---

11. Contact Information

For questions regarding personal data protection, please contact us:

TTN, s.r.o.
Sadová 2719/3A, 905 01 Senica, Slovak Republic
E-mail: **privacy@ttn.sk**
Web: https://ttn.sk