Privacy Policy for Epiteera

Version: 07.10.2026
This Privacy Policy explains how **Kleeo GmbH** processes personal data in connection with the website, the SaaS solution **Epiteera**, customer relationships, support, communication and other business contacts.
This Privacy Policy is not a contract and does not need to be accepted. It serves to inform data subjects.

1 Controller

The controller responsible for data processing is:
Kleeo GmbH
Thurgauerstrasse 105
8152 Glattpark
Switzerland
Email: info@kleeo.ch
Where this Privacy Policy refers to **"we"**, **"us"** or **"our"**, this means Kleeo GmbH.

2 Contact Details of the Swiss Supervisory Authority

Federal Data Protection and Information Commissioner, FDPIC
Feldeggweg 1
3003 Bern
Switzerland
Phone: +41 58 462 43 95

3 Subject Matter of this Privacy Policy

We process personal data to the extent necessary for the operation of our website, the provision of Epiteera, contract performance, communication, security, billing, further development of our services and compliance with legal obligations.
Personal data means any information relating to an identified or identifiable natural person. Epiteera is intended for business customers. Nevertheless, personal data of natural persons may be processed in connection with its use, in particular names, business email addresses, user identifiers, role information and permission information.

4 Applicable Data Protection Law

We are a company based in Switzerland. Our data processing is primarily subject to Swiss data protection law.
To the extent that the General Data Protection Regulation of the European Union, or **GDPR**, applies to certain processing activities, we comply with the corresponding additional requirements.
This may be relevant in particular if we specifically offer products or services to persons in the EU or the EEA or monitor their behaviour.

5 Processing Activities

Depending on how individuals interact with us, we process different personal data for different purposes.

5.1 Visiting our Website

When individuals visit our website, the following data in particular may be processed:

- IP address, used to determine approximate location

- date, time and duration of the visit
- pages viewed and interactions on the website
- referrer URL
- device, browser and operating system information
- pseudonymous identifiers stored in cookies

Subject to consent, we process this data to analyse how our website is used, measure the reach of our content and improve our website. This analysis is carried out using Google Analytics and Google Tag Manager, as described in section 14. The data is processed on a pseudonymous basis and is not used to identify individual visitors.

5.2 Contact by Email or Form

When individuals contact us, request a demo call, complete a form or communicate with us by email, the following data in particular may be processed:

- name
- business email address
- company, optional
- information relating to the enquiry

We process this data in order to respond to enquiries, prepare offers, initiate or maintain business relationships and document our communication.

5.3 Newsletter Sign-Up

When individuals subscribe to our newsletter via the sign-up form on our website, the following data is processed:

- email address
- IP address used at sign-up and confirmation
- date and time of sign-up and confirmation
- whether newsletters are opened and which links are clicked

We process this data in order to send our newsletters, document consent to receive them, and evaluate the reach and effectiveness of our newsletters. Sign-up uses a double opt-in procedure; the IP address, date and time of sign-up and confirmation are stored as evidence of consent. Our newsletters contain a tracking pixel and tracked links that record whether a newsletter has been opened and which links have been clicked. Processing is based on the subscriber's consent. Epiteera's newsletter is sent using MailerLite, a service provided by UAB "MailerLite", Paupio g. 46, LT-11341 Vilnius, Lithuania. The sign-up form is provided by MailerLite, and the data entered is transmitted directly to and stored on MailerLite's servers. Subscribers may withdraw their consent and unsubscribe at any time, via the unsubscribe link included in every newsletter or by contacting **info@kleeo.ch**.

5.4 Use of Epiteera

When using Epiteera, the following data in particular may be processed:

- name
- business email address
- username
- user ID
- Microsoft tenant ID
- role, group and permission information
- administrator status
- login and authentication metadata
- technical usage and log data
- Microsoft 365 configuration information, insofar as it may be personal data
- analysis results, scores, findings and recommendations

- support communication

We process this data in order to provide Epiteera, authenticate users, analyse Microsoft 365 environments, perform Security Health Checks, provide dashboards and recommendations, provide support and ensure the security of the platform.
Epiteera does not read or store the contents of files, emails, chat messages or other customer documents.

5.5 Microsoft 365 and Admin Consent

Epiteera connects to Microsoft 365 environments when an authorised administrator grants the required permissions.
We use these permissions to read and evaluate the configuration data required for the Security Health Check.
The Customer or the authorised administrator may revoke granted permissions via Microsoft administration. Such revocation may result in Epiteera no longer functioning or only functioning to a limited extent.

5.6 Support

When customers request support, we may process in particular the following data:

- name
- business email address
- company
- role or function
- content of the support request
- technical information relating to the request
- affected Epiteera or Microsoft 365 configurations, where required
- communication history

Support is primarily provided by email. For support, task management, documentation or internal collaboration, we may use Microsoft 365 and, where applicable, Atlassian Jira or Confluence.

5.7 Payment, Invoicing and Contract Management

In the case of paid use, depending on the payment method, the following data in particular may be processed:

- name and company
- business email address
- billing address
- contract and order data
- payment status
- invoice numbers
- tax-relevant information
- VAT or UID information
- credit card and payment information via Stripe

For credit card payments, payment information is processed via Stripe. We do not store complete credit card data.
We process this data for contract performance, invoicing, tax calculation, payment processing, accounting and compliance with statutory retention obligations.

5.8 Marketing and Customer Information

We currently use MailerLite for newsletter sign-up, creation and distribution.
We may inform business contacts by email about products, services, news or events, to the extent legally permissible.

Recipients may unsubscribe from marketing communications at any time or inform us that they no longer wish to receive marketing communications.
Transactional messages, for example relating to contracts, security, invoices or support, may continue to be sent.

6 Source of Personal Data

We receive personal data in particular:

- directly from the data subject or their company;
- via forms, emails, meetings or support requests;
- through the use of Epiteera;
- via Microsoft 365 interfaces, insofar as the Customer or an authorised administrator has granted the required permissions;
- from payment service providers;
- from business partners, MSPs or IT service providers, where they use Epiteera for customer mandates.

7 Purposes of Data Processing

We process personal data in particular for the following purposes:

- provision and operation of the website;
- management and deployment of website tags and scripts;
- analysis of website usage and reach, and improvement of our website, subject to consent where required;
- provision, operation and further development of Epiteera;
- authentication and authorisation of users;
- connection to Microsoft 365 tenants;
- performance of Microsoft 365 Security Health Checks;
- creation of dashboards, scores, findings and recommendations;
- customer management;
- communication with prospects, customers and partners;
- sending our newsletter and documenting newsletter consent;
- analysis of newsletter reach and engagement;
- preparation and management of offers;
- contract performance;
- billing, invoicing, tax calculation and payment processing;
- technical support;
- IT security, error analysis and prevention of misuse;
- improvement of our products and services;
- marketing and customer information, to the extent permissible;
- compliance with legal obligations;
- establishment, exercise or defence of legal claims.

8 Legal Bases and Consent

We process personal data within the framework of applicable data protection law, in particular for the performance of contractual and pre-contractual obligations, the protection of legitimate interests, compliance with legal obligations and for permissible business purposes.
We only obtain consent where it is required or appropriate, for example for certain marketing or tracking activities.
Consent given may be withdrawn at any time with effect for the future.

9 Processing on Behalf of Customers

To the extent that we process personal data on behalf of a Customer, we act as a processor.

In this case, our separate Data Processing Agreement applies additionally.
The Customer remains responsible for the lawfulness of processing in its Microsoft 365 environment, in particular for Admin Consent, internal permissions, informing data subjects and compliance with its own legal or regulatory obligations.

10 Recipients and Service Providers

We may disclose personal data to third parties to the extent necessary for the purposes stated. These include in particular:

- hosting and cloud providers;
- newsletter and email marketing providers;
- web analytics and tag management providers;
- payment service providers;
- communication and support tools;
- providers for internal collaboration and documentation;
- accounting, tax and legal advisors;
- authorities, courts or other bodies where we are obliged or entitled to do so;
- business partners where this is necessary for contract performance.

We currently use in particular the following service providers:

Service Provider	Purpose	Place of Processing
Microsoft Azure	Hosting and operation of the Epiteera SaaS application	Switzerland and Europe
Microsoft 365	Email, calendar, Office communication and internal collaboration	according to Microsoft contractual and data protection terms
Stripe	Credit card, invoicing, tax and payment processing for online payments	according to Stripe contractual and data protection terms
Atlassian Jira / Confluence	optional: support, task management, documentation and internal collaboration	according to Atlassian contractual and data protection terms
MailerLite	Newsletter sign-up form, sending of newsletters, management of subscribers and newsletter analysis	European Union; transfers to third countries possible according to MailerLite contractual and data protection terms
Google Analytics	Analysis of website usage and reach, subject to consent	European Union and USA, according to Google contractual and data protection terms
Google Tag Manager	Management and deployment of website tags and scripts	European Union and USA, according to Google contractual and data protection terms

11 Disclosure of Personal Data Abroad

Where possible, we process and store personal data in Switzerland, the EU or the EEA.
The Epiteera SaaS application runs on Microsoft Azure in the EU.
Personal data may be disclosed to other countries, in particular when global service providers such as payment, communication, support, Office or cloud providers are used.
Disclosure abroad only takes place if an adequate level of data protection exists or suitable safeguards are in place, in particular standard contractual clauses or comparable protection mechanisms.

12 Retention Period

We store personal data only for as long as required for the respective purposes.
The retention period depends in particular on:

- contract term;
- statutory retention obligations;
- tax and accounting obligations;
- support and security requirements;
- legitimate evidentiary interests;
- technical backup cycles.

After the end of the contract, we delete personal customer data at the Customer's written request within 60 days, unless statutory retention obligations, legitimate evidentiary interests or technical security obligations prevent deletion.
Data in backups may continue to be stored until the expiry of regular backup cycles, but will not be actively processed unless this is necessary for restoration, security, error analysis or legal obligations.

13 Data Security

We take appropriate technical and organisational measures to protect personal data against unauthorised access, loss, misuse, alteration or disclosure.
These measures include in particular:

- access restrictions;
- role-based permissions;
- authentication and authorisation controls;
- encryption of data transmission, where appropriate;
- protection of the production environment;
- logging of security-relevant events;
- backup and recovery processes;
- patch and vulnerability management.

Despite appropriate measures, absolute security cannot be guaranteed.

14 Cookies and Similar Technologies

We use cookies both on our website at epiteera.io and in the Epiteera application at app.epiteera.io. As the technologies differ, they are set out separately below.

14.1 Epiteera Application

Epiteera uses only technically necessary cookies that are required for the registration and login process. No analysis, tracking or advertising cookies are used.

14.2 Website

Our website uses technically necessary cookies, including a cookie that stores the cookie preferences selected by a visitor. These are set without consent.
Subject to consent, we use Google Analytics and Google Tag Manager, services provided by Google, to analyse website usage on a pseudonymous basis. The cookies set, _ga and _ga_<identifier>, have a storage duration of up to 2 years. Data may be transmitted to Google LLC in the USA. Consent may be withdrawn at any time with effect for the future via the cookie settings on our website.

15 Rights of Data Subjects

Within the framework of applicable data protection law, data subjects may in particular have the following rights:

- access to processed personal data;

- correction of inaccurate personal data;
- deletion of personal data;
- restriction or prohibition of certain processing activities;
- prohibition of certain disclosures to third parties;
- release or transfer of certain personal data;
- objection to certain processing activities;
- withdrawal of consent, where processing is based on consent.

Requests to exercise these rights may be sent to:
info@kleeo.ch
We may require appropriate identification in order to process a request.
Where we process personal data on behalf of a Customer, we generally forward requests from data subjects to the respective Customer registered with Epiteera or process them according to the Customer's instructions.

16 Data Protection Contact

For data protection enquiries, the following contact address may be used:
info@kleeo.ch.

17 EU/EEA Reference and GDPR

We are a company based in Switzerland. Epiteera is primarily aimed at customers in Switzerland. However, customers from the EU or the EEA may also register.
To the extent that the GDPR applies to certain processing activities, we comply with the corresponding additional requirements.
This may be relevant in particular if we specifically offer products or services to persons in the EU or the EEA or monitor their behaviour.
In such cases, data subjects may have additional rights under the GDPR. The respective legal basis may in particular be contract performance, legitimate interests, legal obligations or consent.
We have currently not appointed an EU representative. We regularly review whether such appointment is required.

18 Changes to this Privacy Policy

We may update this Privacy Policy at any time, in particular if our data processing activities, service providers used, legal requirements or services change.
The current Privacy Policy can be accessed at any time at: https://epiteera.io/legal/privacy.html