Privacy Policy

Safety Software | Aktualizacja: 16.12.2025 | https://safetysoftware.eu

Privacy Policy of the Safety Software Application (SaaS)

§1. General information

This Privacy Policy sets out the rules for the processing of personal data by **Safety Software limited liability company** with its registered office in Kraków, at ul. Półłanki 80, 30-740 Kraków, Poland, entered in the National Court Register under KRS number: 0001196649, NIP: 6793342803, REGON: 542821668 (hereinafter: “**Controller**” or “**Company**”).

The Policy has been prepared in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR) and Polish personal data protection regulations.

§2. Scope of application

1. The Policy applies to all personal data processed by the Controller in connection with the use of the SaaS application available at https://safetysoftware.eu (hereinafter: the “Application” or the “Service”) and in connection with conducting commercial communications, customer service, marketing, settlements and cooperation with contractors.

2. The Controller processes data of users who are representatives of entrepreneurs using the Application (hereinafter: “Users” or “Customers”).

§3. Controller details and contact

In matters concerning the processing of personal data, you may contact the Controller by e-mail: **office@safetysoftware.eu** or in writing to: Safety Software Sp. z o.o., ul. Półłanki 80, 30-740 Kraków.

§4. Categories of processed data

The Controller may process the following data:

1. Identification data – first name, last name, position, company name, NIP, contact details (e-mail, phone number).

2. Login and account data – e-mail address, login, password (encrypted), authorisation data.

3. Technical data – IP address, data about the device, browser, login time, activity in the Application.

4. Settlement data – data concerning payments (transaction identifier, payment method, bank account number, card data – to the extent made available by payment operators).

5. Communication-related data – the content of messages sent via contact forms, quotation requests, e-mail correspondence.

6. Marketing data – e-mail address and other data voluntarily provided to receive commercial information (newsletter, remarketing campaigns).

§5. Purposes and legal bases for data processing

The Controller processes personal data for the following purposes and on the following legal bases:

1. **Performance of the contract** for the provision of services by electronic means in the SaaS model (Article 6(1)(b) GDPR).

2. **Financial settlements** and handling payments for the use of the Application (Article 6(1)(b) and (c) GDPR).

3. **Handling enquiries and contacts** (Article 6(1)(f) GDPR – the Controller’s legitimate interest).

4. **Controller’s own marketing**, including sending a newsletter, information about new features and offers (Article 6(1)(a) and (f) GDPR – consent or the Controller’s legitimate interest).

5. **Securing the Application**, detecting abuse, log analysis and maintaining system security (Article 6(1)(f) GDPR).

6. **Compliance with legal obligations** incumbent on the Controller, e.g. accounting or tax obligations (Article 6(1)(c) GDPR).

7. **Maintaining business relationships and cooperation with contractors** (Article 6(1)(f) GDPR).

§6. Voluntariness of providing data

Providing personal data is voluntary, but necessary to conclude and perform the agreement for using the Application or to receive the newsletter and other marketing content. Failure to provide data may prevent the provision of services or the sending of commercial information.

§7. Data recipients

The Controller may disclose personal data to the following categories of recipients:

1. Entities providing payment services – **Stripe Payments Europe Ltd** and **Przelewy24 (PayPro S.A.)**.

2. Entities providing hosting and IT support services.

3. Entities providing accounting and advisory services to the Controller.

4. Providers of analytics and marketing tools, such as **Google LLC** (Google Analytics, Google Search Console), whereby data from Google Fonts and Adobe Fonts are loaded locally from the vendor directory.

5. Public authorities authorised to obtain data under provisions of law.

All entities processing personal data on behalf of the Controller act on the basis of data processing agreements compliant with Article 28 GDPR.

§8. Transfer of data outside the EEA

1. As a rule, the Controller does not transfer personal data outside the European Economic Area (EEA).

2. If such transfer is necessary (e.g. when using tools of providers headquartered outside the EEA), the Controller ensures the application of appropriate safeguards provided for in Article 46 GDPR, in particular standard contractual clauses approved by the European Commission.

§9. Data retention period

1. Data processed for the purpose of performing the contract – for the duration of the contract and for 5 years after its termination (for tax and accounting purposes).

- Marketing data – until consent is withdrawn or an objection to processing is submitted.

- Technical data and logs – for a period of up to 12 months from the date they are recorded.

- Contact data – for the period necessary to provide a response and archive correspondence, no longer than 24 months.

§10. Rights of data subjects

Data subjects have the right to:

1. access their data and obtain a copy thereof,

2. rectification (correction) of data,

3. erasure of data (“right to be forgotten”),

4. restriction of processing,

5. data portability,

6. object to the processing of data on the basis of the Controller’s legitimate interest,

7. withdraw consent to the processing of data at any time (without affecting the lawfulness of processing carried out before the withdrawal of consent),

8. lodge a complaint with the supervisory authority – **the President of the Personal Data Protection Office**.

§11. Data security

1. The Controller applies appropriate technical and organisational measures ensuring the protection of personal data against unauthorised access, loss, destruction or alteration.

2. Access to personal data is granted only to authorised persons who are obliged to maintain confidentiality.

3. The Application system uses secure communication protocols (SSL/TLS) and encrypts users’ passwords.

§12. Cookies and analytics

1. The Service may use cookies to ensure the proper functioning of the Application, traffic analysis, content personalisation and marketing activities.

2. The User may manage cookie settings in their web browser.

3. Analytics tools (Google Analytics, Search Console) are used in the Service to compile statistics and optimise the operation of the website.

§13. Changes to the Privacy Policy

1. The Controller reserves the right to amend this Policy in the event of changes in legal regulations, technology or the scope of activities.

2. The current version of the Policy is published at: https://safetysoftware.eu/PL/p/polityka-prywatnosci.

3. Changes shall take effect on the date of their publication, unless a different effective date is indicated.

§14. Final provisions

1. In matters not governed by this Policy, the provisions of the GDPR and Polish law shall apply.

2. The Policy is effective as of **1 November 2025**

3. In the event of discrepancies between language versions of this Policy, **the Polish version shall prevail**.

Data Controller:
Safety Software Sp. z o.o.

ul. Półłanki 80, 30-740 Kraków, Poland
E-mail: office@safetysoftware.eu
Service: https://safetysoftware.eu