Privacy Policy

Effective date: 20 August 2026

I. General provisions

1. This Privacy Policy sets out the rules on the processing and protection of the Personal Data of Customers and Users (as well as of other persons whose data is processed) in connection with the use of the FerraFlow Platform and of the Services provided within it.

2. The Data Controller is **FERRAFLOW Spółka z ograniczoną odpowiedzialnością** with its registered office in Dzięcioły Dalsze (Dzięcioły Dalsze 63, 08-320 Dzięcioły Dalsze), entered in the Register of Entrepreneurs of the Polish National Court Register kept by the District Court Lublin-Wschód in Lublin with its seat in Świdnik, 6th Commercial Division of the National Court Register, KRS: 0001232717, REGON: 544382368, NIP: 8231677178, share capital PLN 5,000.00 (hereinafter: the "Controller").

3. The Controller may be contacted on data protection matters at the e-mail address office@ferraflow.com and in writing at the address of the Controller's registered office.

4. Personal Data is processed in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR), the Polish Act of 10 May 2018 on the Protection of Personal Data, and other applicable provisions of law.

5. The Controller takes appropriate care to protect the interests of data subjects and, in particular, ensures that data is processed lawfully, for specified, explicit and legitimate purposes, with appropriate security, and that it is adequate and accurate in relation to the purposes for which it is processed.

II. Definitions

Capitalised terms used in this Policy have the meaning given to them in the Terms and Conditions of the FerraFlow Platform, and in addition:

1) **GDPR** – Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

2) **Personal Data** – any information relating to an identified or identifiable natural person.

3) **Data Subject** – a natural person to whom the data relates (in particular the User, a person representing the Customer, or a contact person).

4) **Platform** – the FerraFlow platform, within which the Controller provides the Services.

5) **Policy** – this Privacy Policy.

6) **Terms and Conditions** – the Terms and Conditions of the FerraFlow Platform.

III. Processing of data in connection with the use of the Platform

1. In connection with the User's use of the Platform, the Controller collects data to the extent necessary to provide the individual Services, as well as information on the User's activity on the Platform.

2. Use of the Platform involves sending requests to the server on which the Platform is stored. Every request sent to the server is recorded in the system logs, which may include, among others, the IP

address, the server date and time, and information on the web browser and operating system. As a rule, this data is not associated with specific persons and is used to administer the Platform and to ensure security.

3. Within the Platform, the Controller collects and analyses telemetry data concerning Users' activity, including the history and manner of use of the individual modules, the Assistant and the Tools, the time spent in individual views, the interface elements clicked and the configuration of processes. This data is used to optimise the UX, to provide technical support and to automatically deliver hints and guides facilitating the use of the Platform.

IV. Security of Personal Data

1. The Controller carries out an ongoing risk analysis in order to ensure that Personal Data is processed securely and, in particular, that access to the data is available only to authorised persons and solely to the extent necessary.

2. The Controller applies technical and organisational measures ensuring protection of the processed data appropriate to the risks and to the categories of data, including securing the data against disclosure to unauthorised persons, loss, damage or destruction.

3. Should a Personal Data breach be identified, the Controller takes the actions required by the GDPR, including – where required – notifying the supervisory authority and the data subjects.

V. Purposes and legal bases of the processing

Personal Data is processed for the following purposes and on the following legal bases:

1) creation and servicing of the Account, delivery of the contractual documentation on a durable medium (PDF) and provision of the Services: performance of the contract for the provision of services by electronic means – Article 6(1)(b) GDPR (and, with regard to the data of persons representing the Customer and of contact persons – the legitimate interest, Article 6(1)(f) GDPR, consisting in the performance of the contract concluded with the Customer);

2) handling of orders in the Shop: performance of the contract of sale – Article 6(1)(b) GDPR, and compliance with tax and accounting obligations (including issuing and retaining invoices) – Article 6(1)(c) GDPR;

3) making the Marketplace functionality available and reporting obligations (DAC7): performance of the contract for the provision of the Services – Article 6(1)(b) GDPR, and compliance with a legal obligation to which the Controller is subject as a platform operator with regard to the collection, verification and reporting of sellers' data to the competent tax authorities (the Head of the National Revenue Administration (Szef Krajowej Administracji Skarbowej)) under the provisions on the automatic exchange of information on sellers (DAC7) – Article 6(1)(c) GDPR;

4) analysis of documentation and provision of the Assistant function and the AI Tools: performance of the contract – Article 6(1)(b) GDPR;

5) development, fine-tuning and optimisation of artificial intelligence models and Tools: the legitimate interest of the Controller consisting in improving and developing the Services – Article 6(1)(f) GDPR, with the application of measures minimising the risk to the data subjects (including, as far as possible, anonymisation or pseudonymisation);

6) analysis of Users' activity on the Platform, generation of contextual tips, personalisation of in-app hints, and analytical and statistical purposes: the legitimate interest of the Controller consisting in analysing how the Platform is used in order to improve it – Article 6(1)(f) GDPR;

7) conducting correspondence and telephone contact: the legitimate interest of the Controller consisting in handling enquiries and communication – Article 6(1)(f) GDPR;

8) establishment, pursuit and defence of claims: the legitimate interest of the Controller – Article 6(1)(f) GDPR;

9) handling of complaints and fulfilment of requests relating to data subjects' rights: performance of the contract and compliance with legal obligations, as well as the legitimate interest – Article 6(1)(b), (c) and (f) GDPR respectively;

10) direct marketing, including the sending of commercial information and the Newsletter: consent – Article 6(1)(a) GDPR, in conjunction with the consents required under the Polish Act on the Provision of Services by Electronic Means and the Polish Electronic Communications Law Act (for marketing communication by electronic means and by telephone), and, as regards the Controller's own marketing – the legitimate interest of the Controller, Article 6(1)(f) GDPR;

11) sending technical and organisational communications, educational materials (tutorials) and information on changes to and functions of the Platform as part of implementation support: performance of the contract for the provision of services (Article 6(1)(b) GDPR) and the legitimate interest of the Controller (Article 6(1)(f) GDPR) consisting in ensuring the proper use of the Platform's functions and in building the relationship with the Customer.

VI. Necessity of providing data

1. The provision of Personal Data is voluntary; however, to the extent necessary to conclude and perform the contract (including registration of the Account, handling of orders and compliance with legal obligations) it is a condition for using the Platform or the individual Services. Failure to provide the required data makes it impossible to provide the given Service.

2. To the extent that data is processed on the basis of consent, its provision is voluntary and consent may be withdrawn at any time, without affecting the lawfulness of the processing carried out before its withdrawal.

VII. Social media profiles

1. The Controller may operate profiles on social networking services (e.g. Facebook, LinkedIn). In this connection, it processes the data of persons who visit these profiles or interact with them (e.g. likes, comments, messages), for the purposes of communication, promotion and analysis of activity – on the basis of the legitimate interest of the Controller (Article 6(1)(f) GDPR).

2. The rules on the processing of data by the providers of these services are set out in their own terms and privacy policies. With regard to certain operations, the Controller and the service provider may be joint controllers of the data.

VIII. Recipients of Personal Data

1. In connection with the pursuit of the purposes indicated in this Policy, Personal Data may be disclosed to the following categories of recipients:

1) providers of IT, hosting and cloud infrastructure services and of the maintenance and development of the Platform;

2) providers of artificial intelligence models and services used within the Platform;

3) payment service providers handling payments in the Shop and in the Marketplace;

4) courier companies and carriers – with regard to the delivery of Goods from the Shop;

5) entities providing accounting, tax, legal and audit services;

6) marketing agencies and providers of analytical and marketing tools;

7) public administration authorities, including tax authorities (among others the Head of the National Revenue Administration (Szef Krajowej Administracji Skarbowej) under the DAC7 obligations), where such an obligation arises from provisions of law.

2. Entities processing data on the Controller's behalf do so on the basis of data processing agreements and solely in accordance with the Controller's instructions.

IX. Transfers of data outside the European Economic Area

1. The level of protection of Personal Data outside the European Economic Area (EEA) differs from that ensured by European law. For this reason, the Controller transfers Personal Data outside the EEA only where this is necessary and while ensuring an adequate level of protection.

2. Transfers of data outside the EEA (e.g. in connection with the use of cloud services or AI models supplied by entities from outside the EEA) take place on the basis of a European Commission decision finding an adequate level of protection, or with the application of appropriate safeguards, in particular the standard contractual clauses approved by the European Commission (SCC).

3. Data subjects may obtain a copy of the safeguards applied to transfers of data outside the EEA by contacting the Controller.

X. Automated decision-making and profiling

1. For marketing purposes, the Controller may carry out profiling using analytical and advertising tools (e.g. cookies, Meta Pixel and Google Analytics) to tailor the content and advertisements presented. This profiling does not produce legal effects concerning the persons involved, nor does it otherwise significantly affect them.

2. The Assistant and the AI Tools operate as decision-support systems with human oversight (human-in-the-loop). The results produced by AI have a supporting purpose and do not constitute automated decision-making that produces legal effects concerning data subjects within the meaning of Article 22 GDPR. Final decisions are made by the User.

3. The Controller processes data concerning the User's activity on the Platform in an automated manner (profiling that does not produce legal effects) to display tailored hints, instructions (tutorials) and tips on the optimal use of the Platform's functions. This profiling is based on the Controller's legitimate interest and has the sole supporting purpose of making the Platform easier to use. It does not produce legal effects concerning the User or otherwise significantly affect the User.

XI. Period of processing of Personal Data

1. Data is processed for the period necessary to pursue the purposes indicated in this Policy, in particular:

1) data connected with the Account and with the provision of the Services – for the duration of the contract and, after its termination, for the period necessary to establish, pursue or defend claims (as a rule up to 3 years, unless the law provides for a longer limitation period);

2) data contained in accounting and tax documentation (including invoices) – for the period required by provisions of law, as a rule 5 years counted from the end of the calendar year in which the tax payment deadline fell;

3) data processed in connection with the DAC7 obligations – for the period arising from the applicable tax provisions;

4) data processed on the basis of consent (e.g. marketing, the Newsletter) – until consent is withdrawn;

5) data processed on the basis of a legitimate interest – until an effective objection is lodged or that interest ceases to exist;

6) registration data for Accounts that have not been confirmed via the activation link in the email – for up to 30 days from the date of registration, after which they are permanently deleted;

7) system logs containing users' IP addresses – for a period of 12 months from the date of their recording, for security and technical analysis purposes;

8) data collected by Meta's marketing tools – for a period of 90 days from its recording;

9) data confirming that marketing or other consents have been given – for a period of 3 years from the moment consent is withdrawn or the contractual relationship ends;

10) tokens confirming registration and tokens used to reset a password – for 7 days (registration tokens) and 24 hours (password reset tokens) respectively from the moment they are generated.

2. The retention periods may be extended if such an obligation arises from provisions of law or if this is necessary to establish, pursue or defend claims.

XII. Rights of data subjects

Data subjects have the following rights:

1) the right of access to the data and to obtain a copy of it;

2) the right to rectification (correction) of the data;

3) the right to erasure of the data (the "right to be forgotten");

4) the right to restriction of processing;

5) the right to data portability – to the extent that the data is processed on the basis of consent or of a contract and by automated means;

6) the right to object to processing based on a legitimate interest, including the right to object to processing for the purposes of direct marketing;

7) the right to withdraw consent at any time – without affecting the lawfulness of the processing carried out before its withdrawal;

8) the right to lodge a complaint with the supervisory authority – the President of the Personal Data Protection Office (Prezes Urzędu Ochrony Danych Osobowych).

XIII. Submitting requests relating to the exercise of rights

1. A request concerning the exercise of rights may be submitted to the e-mail address office@ferraflow.com or in writing to the address of the Controller's registered office.

2. If the Controller is unable to identify the person submitting the request on the basis of the information provided, it may ask for additional data in order to confirm the person's identity.

3. A response to the request is provided without undue delay and no later than within one month of its receipt; where necessary, that period may be extended by a further two months, of which the person will be informed.

XIV. Data Protection Officer

The Controller has not appointed a Data Protection Officer. In all matters concerning the processing of Personal Data, the Controller should be contacted in the manner indicated in this Policy.

XV. External links

The Platform and correspondence from the Controller may contain links to other websites that have their own privacy policies. The Controller is not liable for those websites' privacy practices and recommends reviewing their policies.

XVI. Cookies and consent management

1. The Platform uses cookies and similar technologies. Cookies are small text files saved on the User's Device, enabling, among other things, session maintenance, security, traffic analysis and marketing activities.

2. According to their purpose and function, the following categories of cookies are used:

1) **necessary** – required for the proper functioning of the Platform and the provision of the Services; they do not require consent and cannot be disabled;

2) **analytical** – used to analyse how the Platform is used (e.g. Google Analytics 4); applied only after consent has been given;

3) **marketing** – used to present personalised advertisements and for remarketing (e.g. Google Ads, Meta Pixel); applied only after consent has been given.

3. Cookies other than strictly necessary cookies (analytical and marketing cookies) are activated only after the User has given consent through the consent management mechanism (the cookie banner or consent management platform, CMP). Until consent is given, these tools operate in a limited mode in accordance with the Consent Mode mechanism.

4. The User may at any time change or withdraw consent to cookies using the settings available in the banner or in the consent management panel, and may also change the cookie settings in their web browser. Restricting the use of cookies may affect certain functionalities of the Platform.

5. The Controller may use tools supplied by third parties, including Google (Google Analytics 4, Google Ads, Google Tag Manager) and Meta (Meta Pixel), which may use cookies for analytical and marketing purposes, including remarketing. Detailed information on the processing of data by these providers can be found in their privacy policies.

6. The Platform uses analytical and marketing tools supplied by Meta Platforms Ireland Limited (hereinafter: "Meta"). These tools comprise both a script run in the User's browser (Meta Pixel) and a technology for sending events directly from the Platform's server to Meta's servers (Meta Conversions API – CAPI).

7. The transmission of data via the Conversions API (CAPI) takes place in a secure manner, i.e. Users' identifying data (such as the e-mail address) is automatically converted before sending into an encrypted cryptographic hash (SHA-256 standard), making it impossible for unauthorised entities to read the data directly.

8. In connection with the use of the Meta Pixel and the Conversions API, the Controller and Meta Platforms Ireland Limited act as joint controllers of the data with regard to the collection and transmission of data to Meta, in accordance with Article 26 GDPR. The detailed rules of joint controllership, including the allocation of responsibilities, are set out in the Meta Controller Addendum. Further processing of data by Meta for its own advertising purposes takes place on the terms set out in the Meta privacy policy.

XVII. Changes to the Privacy Policy

1. The Policy is verified on an ongoing basis and updated where necessary, in particular in the event of changes in provisions of law, in the scope of the Services provided or in the technologies used.

2. The current version of the Policy applies from 20 August 2026 and is available on the Platform in a manner that allows it to be obtained, reproduced and stored.