PRIVACY POLICY

§ 1. INTRODUCTION

1. This Privacy Policy sets out the rules for the processing and protection of personal data within the Service operated by INNOTEC spółka z ograniczoną odpowiedzialnością with its registered office in Lublin, address: ul. Łużyczan 10/U3, 20-830 Lublin, entered in the Register of Entrepreneurs kept by the District Court Lublin–East in Lublin with its seat in Świdnik, 6th Commercial Division of the National Court Register under KRS number: 0000412990, REGON: 061389016, NIP: 7123270249, share capital: PLN 263,200; e-mail address (hereinafter referred to as the "Controller").
2. Any questions or concerns regarding the processing of personal data may be addressed by e-mail to: privacy@innotec.net.pl.
3. The Controller ensures that personal data entrusted to it by persons using the Service are processed in accordance with generally applicable law, in particular 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 (OJ EU L 119/1), hereinafter referred to as the "GDPR".
4. The Controller's objective is to ensure Users' privacy protection at a level at least equivalent to the requirements arising from applicable law, in particular the GDPR.
5. Any person using the Service accepts all principles set out in this Privacy Policy.
6. The Controller reserves the right to amend this Privacy Policy if required by changes in law or changes in the functionality of the Service. Information on amendments and the date they enter into force will be provided by means of a notice published in the Service.

§ 2. DEFINITIONS

- **User** means a natural person whose personal data are processed by the Controller in connection with the use of the Service.
- **Personal data** means any information relating to an identified or identifiable natural person, including but not limited to first name, last name, identification number, contact details, device IP address, location data, online identifier and information collected via cookies or similar technologies.

- **Service** means the ICT system operated at www.innotec.net.pl, comprising an integrated set of software, databases and related elements (e.g. graphic elements), enabling the provision of services by electronic means.
- **Processing of personal data** means any operation performed on personal data, such as collection, recording, organisation, storage, review, modification, disclosure, erasure or destruction, regardless of whether carried out by automated means or otherwise.
- **Personal data breach** means an incident leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

§ 3. PURPOSES, LEGAL BASES AND SCOPE OF DATA PROCESSING

1. The Controller processes personal data only where at least one of the following conditions applies:
    1. with the User's consent, for the purpose of carrying out activities covered by such consent, including marketing activities (Article 6(1)(a) GDPR);
    2. processing is necessary for the performance of a contract concluded with the User (Article 6(1)(b) GDPR);
    3. processing is necessary for the handling of a complaint, constituting performance of a contract concluded with the User (Article 6(1)(b) GDPR);
    4. processing is necessary for compliance with a legal obligation to which the Controller is subject (Article 6(1)(c) GDPR);
    5. processing serves the purposes of the legitimate interests pursued by the Controller, such as the establishment, exercise or defence of legal claims (Article 6(1)(f) GDPR).
2. The User independently decides on the scope of personal data provided, subject to the fact that failure to provide such data may make it impossible to perform specific services or functionalities available in the Service.
3. Personal data are processed only to the extent necessary to achieve a given purpose and for no longer than permitted by applicable law.

§ 4. DATA SECURITY

1. The Controller regularly conducts risk analyses in order to identify threats related to the processing of personal data and implements appropriate technical and organisational measures to ensure their security.
2. The Controller ensures that access to personal data is granted only to persons authorised by the Controller and solely to the extent necessary to perform the tasks entrusted to them. Authorisations are granted individually and documented.
3. The Controller maintains a register of persons authorised to process personal data. Such persons are obliged to maintain strict confidentiality of both the data themselves and the methods used to secure them, also after termination of cooperation with the Controller.
4. Personal data are protected against unauthorised access, modification, loss or destruction by applying, among others:
    1. encryption of data transmission,
    2. server security measures,
    3. role-based access restrictions,
    4. access control procedures and audit of data operations.
5. The Controller's IT systems are monitored for security breaches and are subject to regular updates and testing.
6. In the event of a personal data breach, the Controller implements procedures enabling rapid assessment of the scale of the incident and, where required, notifies the competent supervisory authorities and data subjects in accordance with applicable law.
7. The Controller uses the services of trusted external providers offering cloud-based solutions. The processing of personal data within such services takes place solely on the basis of agreements ensuring compliance with applicable law, including the GDPR, and with the application of appropriate security mechanisms and access controls.
8. In order to ensure continuity of the Service and protect data against loss, the Controller performs regular backups of personal data. These backups are stored in secure locations with the use of technical and organisational measures preventing unauthorised access. The retention period of backups is adjusted to the nature of the data and the purpose of processing.

§ 5. DATA RECIPIENTS

1. Recipients of Users' personal data may include entities cooperating with the Controller that have been entrusted with activities requiring data processing, in particular in the areas of e-mail services, hosting, ICT and IT services, as well as administrative, legal and advisory support.
2. External entities having access to personal data process them solely on the basis of a personal data processing agreement and exclusively on the Controller's instructions.
3. Users' personal data may also be disclosed to public bodies or authorities authorised to receive them, only in justified cases and on the basis of generally applicable law.

§ 6. RECEIPT OF COMMERCIAL INFORMATION

The User may, if the Service provides such an option, consent to receiving commercial information by electronic means. Such consent may be withdrawn at any time, without giving reasons, by sending an appropriate request to the Controller's e-mail address.

§ 7. USERS' RIGHTS

1. Any person whose data are processed has the following rights:
    1. the right of access to data and information on their processing (Article 15 GDPR). The Controller provides information on the processing, including purposes, legal bases, scope of data, recipients and the planned date of erasure, and makes available the personal data covered by the request;
    2. the right to obtain a copy of the data (Article 15(3) GDPR). The data subject who submits such a request has the right to receive a copy of the processed data, provided that this does not adversely affect the rights of third parties and is technically feasible;
    3. the right to rectification (Article 16 GDPR). The data subject may request correction of inaccurate data as well as completion or updating where data are incomplete or have changed;
    4. the right to erasure ("right to be forgotten") (Article 17 GDPR). The data subject may request erasure of data that are no longer necessary for the purposes for which they were collected;

5. the right to restriction of processing (Article 18 GDPR). The Controller restricts processing operations other than storage where the data subject requests restriction or where such obligation arises from the legal situation (e.g. due to pending administrative proceedings);
6. the right to data portability (Article 20 GDPR). The data subject has the right to receive their data in a structured format and to transmit them to another controller;
7. the right to object to processing for purposes other than marketing (Article 21 GDPR). The data subject may object to such processing; the objection is subject to assessment by the Controller;
8. the right to object to processing for marketing purposes (Article 21(2) GDPR). The data subject may object at any time to the processing of personal data for marketing purposes, without the need to justify the objection;
9. the right to withdraw consent (Article 7(3) GDPR). Where processing is based on consent, the data subject may withdraw it at any time; this does not affect the lawfulness of processing carried out before withdrawal;
10. the right to lodge a complaint (Article 77 GDPR). Where the data subject considers that the processing of personal data infringes the GDPR or other data protection provisions, they may lodge a complaint with the supervisory authority, namely the President of the Personal Data Protection Office of Poland (https://uodo.gov.pl/pl/p/kontakt).

2. A request regarding the exercise of data subject rights may be submitted:
    1. in writing to the Controller's registered office address;
    2. electronically to the Controller's e-mail address.
3. A response will be provided within one month of receipt of the request. If an extension is necessary, the Controller will inform the applicant of the reasons for the delay.
4. The response will be sent to the e-mail address from which the request was submitted, and in the case of requests submitted by post, by registered mail to the address indicated by the applicant.

§ 8. COOKIES AND SIMILAR TECHNOLOGIES

1. The Service uses cookies and other similar technologies (e.g. local storage, tracking pixels) to ensure the proper functioning of the Service, analyse traffic and tailor content to the User's preferences.
2. Cookies are IT data stored on the User's end device. They are used in particular to:
    - maintain the session after login,
    - remember settings and preferences,
    - collect statistical data,
    - conduct analytical and marketing activities, exclusively with the User's consent.
3. Web browsers usually allow cookies to be stored on the User's end device by default. The User may at any time manage browser settings, including limiting or completely blocking cookies. Such restrictions may, however, affect the functionality of the Service.
4. The Controller cooperates with external service providers whose list may change. These entities may use cookies for the purpose of:
    - monitoring traffic in the Service,
    - preparing aggregated and anonymous statistics,
    - controlling the frequency of content or advertisement displays,
    - analysing the effectiveness of newsletter subscriptions,
    - communicating with the User (e.g. via chat),
    - integration with social media platforms.
5. Detailed information on cookies used and methods of managing them is available in browser settings and in the Cookie Policy.
6. The Controller may use Google Analytics to analyse statistics. In such a case, the User's data may be transferred to Google LLC (1600 Amphitheatre Parkway, Mountain View, CA 94043, USA). The User may block access to their data by installing the plug-in available at https://tools.google.com/dlpage/gaoptout.
7. The Controller encourages Users to review details of data processing by Google Analytics available at: https://policies.google.com/privacy?hl=pl.

§ 9. SERVER LOGS

1. Use of the Service website involves sending requests to the server on which it is hosted. Each such request is automatically recorded in server logs.
2. Logs include, among others, the User's IP address, the date and time of the request, and information on the web browser used and the operating system. These records are stored exclusively on the server.
3. Data contained in logs are not linked to specific individuals and are not used by the Controller to identify the User.
4. Server logs constitute auxiliary material used solely for the management and maintenance of the Service and for the analysis of its security. Access to them is granted only to persons authorised to maintain the server infrastructure.
5. Data contained in server logs may also be used in the event of suspected actions compromising the security of the Service, including unauthorised access attempts. Such information may be used to analyse the incident, determine its causes and implement remedial measures. Where justified, it may be disclosed to law enforcement authorities or other entities authorised under applicable law.

§ 10. TRANSFER OF DATA OUTSIDE THE EEA

1. As a rule, the Controller does not transfer personal data outside the European Economic Area (EEA). If such a transfer occurs, it is made exclusively to third countries or entities in respect of which the European Commission has issued an adequacy decision confirming an adequate level of personal data protection (Article 45 GDPR).
2. The current list of third countries recognised by the European Commission as ensuring an adequate level of data protection is available at: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

§ 11. AUTOMATED DECISION-MAKING AND PROFILING

1. Within the Service, the Controller may process the User's personal data in an automated manner in order to tailor the content presented, including informational messages and advertisements, to the User's preferences and interests. Such processing may include profiling, consisting in the automated analysis of User data (e.g. activity on the Controller's websites) in order to assess the User's interest in the Controller's services.

2. Profiling used by the Controller serves exclusively informational and marketing purposes, consisting in tailoring content to the User's predicted interests. It does not lead to automated decisions producing legal effects or otherwise significantly affecting the User's personal, professional or financial situation within the meaning of Article 22 GDPR.
3. The User has the right to object at any time to the processing of their personal data for profiling purposes, in particular for marketing purposes, in accordance with Article 21(1) GDPR. The objection may be submitted by sending an appropriate request to the Controller's contact address indicated in this Policy.
4. Where technically available, the User may also object by changing account settings or using tools enabling the management of marketing consents available in the Service.

§ 12. AMENDMENTS TO THE PRIVACY POLICY

1. The Controller reserves the right to amend this Privacy Policy, in particular in the event of:
    - changes in applicable personal data protection law,
    - implementation of new services, functionalities or technologies in the Service,
    - the need to adapt the document to guidelines of supervisory authorities.
2. The amended Privacy Policy will be published on the Service website together with the effective date.
3. Users will be informed of material changes to the Policy by means of an appropriate notice published in the Service or sent directly, where contact details are available and required by law.
4. Continued use of the Service after the effective date of the amendments constitutes acceptance of the updated Privacy Policy.

§ 13. FINAL PROVISIONS

1. In matters not regulated by this Privacy Policy, generally applicable provisions of law shall apply, in particular:
    - Regulation (EU) 2016/679 of 27 April 2016 (GDPR),
    - the Act of 10 May 2018 on the protection of personal data,

- the Act of 18 July 2002 on the provision of services by electronic means,
- the Act of 12 July 2024, Electronic Communications Law.

2. Any questions, comments or requests regarding the processing of personal data should be addressed to the Controller using the contact details indicated in the “Introduction” section or on the Service website.
3. This Privacy Policy is effective as of 1 January 2026.