Annex No. 2 to the Terms and Conditions for the Provision of the “ENNO-EMS” Application Usage Service by Ennovation Technology Sp. z o.o.

ENNO-EMS Privacy Policy

Terms capitalized herein shall have the meanings assigned to them in the Terms and Conditions for the Provision of the “ENNO-EMS” Application Usage Service by Ennovation Technology.

General Provisions

This Privacy Policy is intended for Users visiting the website https://ennovationtech.eu/system-zarzadzania-energia-ems/ and using the "ENNO-EMS" application service provided by Ennovation Technology.

This Privacy Policy has been developed based on the provisions of the GDPR, the Personal Data Protection Act, and other applicable national laws, in order to ensure the highest level of personal data protection and the security of information processed by the Controller. This document complies with best practices in data security management, taking into account international standards as well as national regulations regarding personal data protection and IT security.

This Privacy Policy applies to all information systems, data processing activities, applications, and IT infrastructure used by the Controller, as well as to external entities involved in data processing. It also applies to individuals associated with the Controller, such as employees, collaborators, business partners, subcontractors, and service providers.

Definitions

Controller – ENNOVATION TECHNOLOGY sp. z o.o., with its registered office at ul. Baletowa 14, 02-867 Warsaw, registered in the Register of Entrepreneurs maintained by the District Court for the Capital City of Warsaw, 14th Commercial Division of the National Court Register under KRS no. 0000760282, NIP: 1132989675.

Personal Data – any information relating to an identified or identifiable natural person. This means data that allows for direct or indirect identification of a person, such as: name, surname, residential address, telephone number, email address, PESEL number, IP address, location data, and other information which, when combined with other data, can lead to identification.

Incident – an event resulting in accidental or unlawful disclosure, destruction, loss, alteration, or unauthorized access to personal data. The Controller is obliged to manage such incidents appropriately, including logging, analyzing, and undertaking corrective actions in accordance with applicable procedures and legal regulations, particularly the GDPR.

Data Protection Officer (DPO) – a person appointed by the Controller to oversee compliance with personal data protection laws within its operations. The DPO is responsible for fulfilling the duties outlined in Article 39 of the GDPR, including monitoring the lawfulness of processing, implementing appropriate data protection measures in electronic communication, training staff, and cooperating with supervisory authorities such as the President of the Personal Data Protection Office (PUODO).

PKE – the Act of 12 July 2024 – Electronic Communications Law (Journal of Laws 2024, item 1221).

Cookies – files used to store information related to the operation of the website, such as user preferences, browsing history, or login data. Depending on their type, the use of cookies may require the user's consent.

Data Subject/User – a natural person whose personal data is processed by the Controller. The data subject has certain rights under the law, including the right to object to the processing of their data for marketing purposes, the right to access their data, to rectify or erase it ("the right to be forgotten"), and other rights granted under applicable law, especially the GDPR.

Policy – this document, setting out the rules for processing and protecting personal data within the activities of the Controller, prepared in accordance with applicable legal regulations, in particular Regulation (EU) 2016/679 (GDPR) and the Electronic Communications Law (PKE).

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, repealing Directive 95/46/EC.

Application – software provided as part of the Service, enabling the collection, processing, and management of data from technical installations used by the User.

User Consent – a freely given, specific, informed, and unambiguous indication of the user's will by which they agree to the processing of their personal data, including for marketing purposes and the use of tracking technologies.

Objectives of the Privacy Policy

The purpose of this Policy is to minimize risks associated with the processing of personal data and to ensure the confidentiality, integrity, and availability of information. The Policy includes risk identification, implementation of protective measures, and monitoring compliance with legal regulations. It takes into account the requirements of the GDPR, the Electronic Communications Law (PKE), and national laws, including the Personal Data Protection Act and regulations on electronic communications security. The Controller commits to complying with applicable legal regulations and to regularly reviewing them. The Controller has implemented appropriate technical and organizational measures aimed at protecting IT systems from both external and internal threats, ensuring their uninterrupted operation and compliance with current legal regulations. The Controller adopts a comprehensive approach to managing risks related to the processing of personal data, including their identification, assessment, and mitigation. A key element is ensuring the continuity of IT systems, including contingency planning, incident management, and disaster recovery procedures.

Personal Data Protection Principles

Personal data is processed only to the extent necessary to achieve specific purposes, in accordance with the principle of data minimization, limiting data collection to the minimum required. The Controller processes personal data lawfully and transparently, basing each process on an appropriate legal basis, such as consent, contract, legal obligation, or legitimate interest.

The Controller maintains documentation of data processing activities, including records of processing activities and risk assessments, ensuring compliance with legal regulations.

Scope of Data Collected

During a visit to the Controller's website, data related to the User's activity is automatically collected, such as time spent on the site, search queries, number of subpages viewed, date and source of the visit, IP address, domain name, and type of web browser. The User may provide data to register a User Account in the Application. The registration form requires the provision of identification and contact details necessary for using the User Account and for the provision of services by the Controller. The User may also voluntarily provide additional data. The User Account will store information about the selected Package, payment history, and complaints. The Application does not allow access to the Service without registering a User Account. The Application allows contact with the Controller, whereby the User may provide identification and contact information as well as details related to the content of the message. With the User's consent, contact and/or analytical data may be collected for marketing purposes, including sending promotional offers or information about new products and services.

Purposes and Legal Basis for Personal Data Processing

The Controller processes personal data for the following purposes:

Analysis of network traffic, ensuring security within the Application, and tailoring content to the needs of Users on the basis of the Controller's legitimate interest (Article 6(1)(f) of the GDPR);

Providing responses to submitted questions and conducting correspondence in order to resolve matters, on the basis of consent and the Controller's legitimate interest, which is to fulfill requests and provide Services to Users (Article 6(1)(a) and (f) of the GDPR);

Establishing and using a User Account in the Application on the basis of a contract for the provision of electronic services concluded with the User, as the service recipient (Article 6(1)(b) of the GDPR);

Handling complaints, on the basis of the Controller's legitimate interest (Article 6(1)(f) of the GDPR);

Promotion of goods and services or sending offers, based on the User's consent (Article 6(1)(a) of the GDPR);

Debt collection in the event of non-payment for services provided by the Controller (Article 6(1)(f) of the GDPR);

Transfer of personal data to Santander Bank Polska S.A., with its registered office in Warsaw, at al. Jana Pawła II 17, 00-854 Warsaw ("Bank"), in connection with:

The provision by the Bank to the Controller of a service enabling infrastructure for handling Internet payments (Article 6(1)(f) of the GDPR),

The handling and settlement by the Bank of payments made by Users via the Internet using payment instruments (Article 6(1)(f) of the GDPR),

In order to verify by the Bank the proper execution of contracts concluded with the User, in particular ensuring the protection of payers' interests in relation to complaints submitted by them (Article 6(1)(f) of the GDPR);

Providing the data is voluntary but necessary. Failure to provide the data will accordingly prevent the provision of the Service, the creation of a User Account, handling of complaints, receiving an offer or ordered marketing materials, or receiving a response to a submitted inquiry.

Providing data necessary for the statistical analysis of Application Users is voluntary. One may use so-called incognito mode to browse the website without sharing visit information with the Controller. Using incognito mode—thus not providing the data—does not affect the possibility of using the Application via a browser.

User Rights

The Controller ensures the ability to exercise the rights of Data Subjects in accordance with the principles set out in the GDPR, including:

The right to obtain information about the purposes, legal bases, scope of processed data, recipients, and data retention periods.

The right to receive a copy of the processed personal data.

The right to rectify or supplement inaccurate or incomplete personal data.

The right to erase or anonymize data that is no longer necessary for the purposes for which it was collected.

The right to request the restriction of data processing, except where the data must be retained in accordance with the retention policy or based on a decision of a supervisory authority.

The right to receive personal data in a commonly used format that allows for its transfer to another controller.

The right to object to the processing of their data for marketing purposes.

The right to object to processing based on the Controller's legitimate interest, if there are special circumstances.

The right to withdraw consent to data processing at any time, without affecting the lawfulness of the processing carried out before the withdrawal.

Sharing and Commissioning the Processing of Personal Data

Personal data may be shared with other controllers only when the requirements of the GDPR are met. The Controller carefully verifies the legal grounds before disclosing any data.The commissioning of personal data processing is carried out on the basis of a data processing agreement, in accordance with Article 28 of the GDPR, which defines the purpose, scope of processing, and appropriate data protection measures.

Before commissioning the processing of data, the Controller verifies whether the processor meets security requirements and applies appropriate data protection measures, ensuring compliance with the GDPR.

Data Retention

Data is retained only for the period necessary to fulfill the purposes of processing, after which it is deleted or archived in accordance with applicable legal provisions. Personal data shall be retained as follows:
In the case of a User Account registration, for the duration of account use; after account closure, the Controller shall retain billing data for five (5) years following the year in which the tax obligation related to the order arose;
For settlement-related data, for five (5) years following the year in which the tax obligation related to the Agreement arose;
Until the withdrawal of consent or resolution of the matter, and thereafter until the expiration of the limitation period for any claims arising from such processing;
For complaints, until the expiration of the limitation period for potential claims;
Data related to traffic analysis collected via cookies and similar technologies may be retained until the expiration of the respective cookie. Certain cookies do not expire, in which case the data retention period shall correspond to the time necessary for the Controller to fulfill the purposes of collection, such as ensuring security and analyzing historical traffic data.
The Controller applies regular verification procedures to limit data storage to the necessary minimum. Upon expiration of the specified period, data is deleted or archived.
Automated systems monitor data retention periods and initiate deletion processes upon the expiry of the established deadlines, ensuring compliance with the data minimization principle outlined in Section 3.1.
Data concerning electronic communications, including traffic data and metadata, is retained in accordance with the requirements of the Electronic Communications Law (PKE) and only in circumstances necessary for the realization of objectives defined by applicable legislation.

Transfer of Data to a Third Country

In accordance with applicable legal regulations, Users' personal data shall not be transferred to third countries (outside the territory of the European Union and the European Economic Area) or to international organizations, unless such an obligation arises from legal provisions or the User has given explicit consent.

The Controller takes all necessary measures to protect personal data and does not transfer it to countries that do not provide an adequate level of personal data protection as defined by European law, including the GDPR.

In the event of a change in the legal situation that may affect the manner in which personal data is processed—particularly if it results in the need to transfer data to a third country—the Controller shall promptly inform the User.

Cookies

The browser-based version of the Application uses cookies and similar technologies to collect information about the User. Their use involves storing data on the User's device (e.g., computer, smartphone). Cookies are used to:

Remember User preferences (e.g., font size, contrast settings, acceptance of the privacy policy),

Maintain the User's session (e.g., after login),

Remember the password (with explicit consent),

Ensure security (e.g., detect abuse),

Analyze visits and tailor content.

Information collected via cookies is not linked to other User data within the Application and is not used to identify the User.

The User may:

Configure their browser to block specific types of cookies or limit their use to essential ones only,

Change browser settings at any time or delete stored cookies,

Use the website in incognito mode, which blocks data collection related to their visit.

By default, most browsers accept all cookies. Detailed information on managing cookies can be found in the browser's settings.

The Application uses the following categories of cookies:

Essential – contribute to the usability of the website by enabling basic functions such as page navigation and access to secure areas of the site. The website cannot function properly without these cookies.

Preference – allow the website to remember information that changes the way it behaves or looks, such as the User's preferred language or the region they are in.

Statistical – help the Controller understand how different Users interact with the site by collecting and reporting anonymous information.

Marketing – used to track Users across websites. The aim is to display ads that are relevant and engaging for individual Users and therefore more valuable for publishers and third-party advertisers.

Cookies used for marketing and statistical purposes are applied only with the User's explicit and voluntary consent. Consent is collected through appropriate tools available on the Website.

Blocking or limiting cookies may affect the functionality of certain features of the Websit

Incidents management

The security policy includes a detailed incident management plan that defines procedures for identifying security incidents, classifying them, assessing risks, taking remedial actions, reporting, and preventing future breaches.

In the event of an Incident, the Controller shall promptly take the following steps:

Analyze the scope and nature of the incident to mitigate its effects;

Notify the data subjects about the incident and the measures taken to protect their data, as well as indicate possible consequences and recommended protective actions;

Conduct internal audits to draw conclusions and minimize the risk of similar events in the future;

Report the breach to the relevant supervisory authority (President of the Personal Data Protection Office) within 72 hours of discovering the incident, unless the breach does not pose a risk to the rights or freedoms of natural persons. The report includes a description of the nature of the breach, the categories and approximate number of affected individuals, possible consequences of the breach, and the measures taken to address it.

The Controller implements and continuously improves safeguards against cyber threats, including:

Intrusion Detection and Prevention Systems (IDS/IPS),

Regular updates and security patches,

Encryption of data in transit and at rest,

Network traffic monitoring to detect suspicious activity,

Implementation of data access minimization principles,

Regular security audits and reviews,

Employee training in incident response,

Procedure testing through incident simulations,

Automated and manual security testing of the application and infrastructure.

The Controller pays special attention to protection against electronic communication threats such as DDoS attacks, ransomware, phishing, and unauthorized data access.

Final Provisions

In all matters related to personal data protection, the Controller provides the opportunity to contact the Data Protection Officer. Contact is possible via the following email address: inspektor@ennovationtech.eu.

In matters not regulated by this Policy, the provisions of the Civil Code and applicable Polish laws, as well as European Union law, in particular the 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, repealing Directive 95/46/EC), shall apply.

This Policy is effective as of May 1, 2025. Users will be informed of any changes to the Policy through its re-publication in the Application and by means of an appropriate notice.