

## INTRODUCTION

PannonWatt Zrt. (hereinafter: Service Provider, Data Controller, Company), as Data Controller, acknowledges the content of this legal notice as binding on itself.

PannonWatt Zrt. reserves the right to change this information at any time. Naturally, it will inform its audience in good time of any changes.

PannonWatt Zrt. is committed to protecting the privacy of its guests and partners, and it is of utmost importance to respect its customers' right of informational self-determination. The Data Controller shall treat personal data confidentially and shall take all security, technical and organizational measures that guarantee the security of the data.

PannonWatt Zrt. describes its data management principles below, outlines the expectations it has set for itself and which it adheres to as a Data Controller. PannonWatt Zrt. privacy policy is in accordance with applicable data protection law, in particular:

- Act CXII of 2011 - on the right to self-determination and freedom of information;
- Act V of 2013 - on the Civil Code (Ptk.);
- Act C of 2000 on Accounting (Számv. tv);
- EU Regulation 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 (General Data Protection Regulation, hereinafter "**GDPR**")

## 1. DEFINITIONS

- 'data subject' means any natural person directly or indirectly identified or identifiable on the basis of personal data;
- 'personal data' means any information relating to the data subject, in particular name, identification number, or to one or more factors specific to the physical, physiological, mental, economic, cultural or social identity of that natural person; and the conclusions relating to the data subject drawn from these;
- 'consent' of the data subject means any voluntarily given, specific, informed and unambiguous indication of the data subject's wishes by which he or she signifies agreement to the processing of personal data (complete or to a specific action) relating to him or her;
- 'data controller' means the natural or legal person, or any entity without legal personality who or which, alone or jointly with others, determines the purposes of the processing of personal data, makes and implements the data management (including the means used), or executes with the data processor;
- 'data management' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, registering, structuring, storage, alteration, use, retrieval, transfer, disclosure, alignment or combination, restriction, erasure or destruction; furthermore to prevent future use of the data, taking photographs, sound or images and recording physical characteristics (e.g. fingerprints, palmprints, DNA samples, iris images) of the person;
- 'data transfer' is when data is made available to a specific third party;
- 'disclosure' means making information available to anyone;

- 'erasure of data' means making data unrecognizable in such a way that it is no longer possible to recover it;
- 'data processing' means any technical operation which is performed on personal data, irrespective of the method and means used to perform the operations and the place of application, provided that the technical operation is performed on the data;
- 'data processor' means any natural or legal person, or any entity without legal personality, who or which carries out the processing of data on the basis of a contract, including a contract under a legal provision.

## 2. COMPANY DATA

Our company details and contact details are as follows:

Company name:	PannonWatt Zrt.
Headquarters:	H-9027 Győr, Kandó Kálmán út 11-13.
Company Registration Number:	08 10 001892
Tax number:	25327292-2-08
Phone number:	+36 1 245 4567
E-mail:	office@pannonwatt.hu
Data Controller Representative:	VÓNEKI Róbert – Chief Executive Officer

**3. PERSONAL DATA, PURPOSE, LEGAL BASIS AND DURATION OF THE PROCESSING** We would like to draw the attention of those who provide data to PannonWatt Zrt. that if they do not provide their own personal data, it is the duty of the data provider to obtain the consent of the data subject.

We provide the following information regarding each of our data management activities.

### 3.1. Request for quotation, direct inquiry

Those interested may contact the Company directly by e-mail at office@pannonwatt.hu or by telephone.

**Purpose of data management:**

Keeping in touch with each other in order to facilitate communication between the data subject and our Company and to work as closely and efficiently as possible.

**Legal basis** for the data management: legitimate interest, - Article 6 (1) (f) of the GDPR

**Personal data managed:** Name of contact person; e-mail address, phone number or other information provided by the data subject

**Duration of data management:** until the data subject objects, or the purpose of data management is achieved

**Recipients of personal data:** Controlled data will not be disclosed by the Data Controller to any third party other than the data processor (s) referred to in point 8. Records may only be accessed by Data Controller as well as employees and designated colleagues of the data processor (s).

**Identification of a legitimate interest:** It is in the legitimate interest of our Company to manage the data provided by the data subject - as a direct business acquisition.

**Possible Consequences of Failure to Provide Data:** Communication between the data subject and the Company is not possible or limited.

**Data subjects involved in data management:**

Partners and data subjects directly interested in the Company's services (e.g. by e-mail, telephone).

### 3.2. Order, data management related to the fulfillment of the contract

**Purpose of data management:** customer registration, fulfillment of orders, contracts, keeping in contact with contractual tasks.

**Legal basis for data processing:** voluntary consent of the data subject - - Article 6 (1) (a) GDPR

**Personal data managed:** Contact name and first name; telephone number; e-mail address; unique identifier, other information provided by the data subject

**Duration of data management:** until the fulfillment of the contract / order, or the documents related to

contract performance shall be retained for 8 years

**Possible Consequences of Failure to Provide Data:** Providing information is not a prerequisite for contracting, and is not required to provide personal information. Failure to provide data may make communication difficult.

**Recipients of personal data:** Controlled data will not be disclosed by the Data Controller to any third party other than the data processor (s) referred to in point 7. Records may only be accessed by Data Controller as well as employees and designated colleagues of the data processor (s).

**Data subjects involved in data management:**

Partners and data subjects having contractual relationship with PannonWatt Zrt.

### 3.3. Invoice issuance (in case of a natural person)

**Purpose of data management:** issuing an invoice to the payer, complying with legal requirements

**Legal basis for data management:** by law - Act C of 2000 Section 166 (1)

**Personal data managed:**

- Name of the bill payer
- Billing address
- Amount
- Billed Services

**Duration of data management:** by the deadline specified in Act C of 2000 on Accounting Section 169 (2)

**Possible Consequences of Failure to Provide Data:** Provision of data is a legal obligation.

**Recipients of personal data:** Controlled data will not be disclosed by the Data Controller to any third party other than the data processor (s) referred to in point 7. Records may only be accessed by Data Controller as well as employees and designated colleagues of the data processor (s).

**Data subjects involved in data management:**

Data subjects for whom the Data Controller issues an invoice.

## 4. OTHER DATA MANAGERMENTS

Data handling not listed in this brochure will be provided at the time of data collection. We inform our clients that certain authorities, public authorities and courts may contact our Company for personal information. Our Company will provide such bodies with personal data only to the extent necessary to fulfill the purpose of the request, provided that the purpose and scope of the request are specified by the relevant authority and if the execution of the request is required by law.

## 5. CHILDREN

Our services are not intended for persons under the age of 16 and we ask persons under the age of 16 to not provide personal data to the data controller. If we become aware that we have collected personal information from a child under the age of 16, we will take the necessary steps to delete the information as soon as possible.

## 6. RELEASE OF PERSONAL DATA TO A THIRD COUNTRY OR TO AN INTERNATIONAL ORGANIZATION

Our company will not directly transfer your personal information above to any third country or international organization.

## 7. INFORMATION CONCERNING THE USE OF THE DATA PROCESSOR

During the processing, the Data Controller shall forward the data to the data processor (s) contracted to perform the contract.

**Recipient categories:** accounting / bookkeeping service provider, IT system operator, web hosting provider

The Data Processors employed are recorded in the Company's internal records.

## **8. METHOD OF STORING PERSONAL DATA, SECURITY OF DATA MANAGEMENT**

Our computer systems and other data storage locations are located at the headquarters and on servers provided by the data processor. Our Company selects and operates the IT tools used to manage your personal information in the course of providing the service in such a way that the managed data:

- a) accessible to those entitled (availability);
- b) its authenticity and authentication are assured (authenticity of data management);
- c) its invariance can be demonstrated (data integrity);
- d) is protected against unauthorized access (data confidentiality).

We pay particular attention to the security of the data and take the additional technical and organizational measures and procedures necessary to enforce the GDPR warranties. In particular, the data shall be protected by appropriate measures against unauthorized access, alteration, transmission, disclosure, deletion or destruction, and against accidental destruction, damage or unavailability due to technological cut-over performed.

Both our company and our partners' IT systems and networks are protected against computer-assisted fraud, computer viruses, computer hacking and denial of service attacks. The operator also provides security through server-level and application-level security procedures. Data backup is accomplished daily. In order to avoid privacy incidents, our company will take all possible measures; however, in the event of such an incident, we will take immediate action to minimize the risks and prevent damage, in accordance with our incident management policy.

## **9. RIGHTS OF DATA SUBJECTS, REMEDIES**

The data subject may request information on the processing of his or her personal data, and may request the rectification, deletion, cancellation of his or her personal data, except for mandatory data processing, and may exercise his or her right to data portability and objection as indicated at the time of recording or to the above contact details of the Data Controller.

The rights and remedies of the data subject under Act CXII of 2011 and the EU Regulation 2016/679 are set out and communicated to the parties concerned as follows.

The right of information, also known as the "right of access" of the data subject: The Data Controller shall, upon request of the data subject, provide information in accordance with the provisions of Act CXII of 2011 and Article 15 of EU Regulation 2016/679 on

- the data and categories of personal data that it processes,
- the purpose of data management,
- the legal basis for data management,
- duration of data management,
- where appropriate, the period for which the data will be stored or, where this is not possible, the criteria for determining this period,
- where applicable, if the data were not collected from the data subject, of any available information as to their source,
- where appropriate, the use of automated decision-making, including profiling, and the logic and intelligible information about the importance of such data management and the expected consequences for the data subject;
- the data of the data processor, if a data processor has been used, or the circumstances, the effects of the privacy incident, and the measures taken to address it; and
- in case of transfer of personal data of the data subject, the legal basis, purpose and recipient of the transfer.

The information shall be provided free of charge if the person requesting the information has not yet submitted an information request to the Data Controller for the same scope of data in the current year. In other circumstances the costs already paid must be refunded. Reimbursement of costs already paid shall be refunded if the data have been unlawfully processed or the request for information has led to

a correction.

6. The Data Controller draws the attention of those concerned that the information should be denied in accordance with Act CXII of 2011

a. if the Data Controller receives personal data pursuant to a law, an international treaty or a binding act of the European Union, and the data transferring data controller indicates, at the same time as the data is transferred, the restriction or other limitations on the rights of the personal data subject pursuant to the Act mentioned above.

b. in view of the external and internal security of the State, such as national defense, national security, the prevention or prosecution of crime, the security of law enforcement, the economic or financial interests of the State or local authorities, moreover, for the purposes of protecting the economic or financial interests of the European Union, and preventing and detecting disciplinary and ethical misconduct in connection with the exercise of the profession and breaches of labor law and safety, including in all cases monitoring and surveillance, and for the protection of the rights of the data subject or of others.

The Data Controller shall notify the National Data Protection and Freedom of Information Authority of the rejected requests for information by 31 January of the year following the reference year.

Right of rectification: The data subject shall have the right to rectify any inaccurate personal data concerning him or her upon his or her request without undue delay. Given the purpose of the data processing, the data subject shall have the right to request that personal data which are incomplete be completed, including by means of a supplementary declaration. However, if the personal data do not correspond to the reality and the correct personal data are available to the Data Controller, the latter is obliged to correct the personal data without the request of the data subject.

Right to erasure, also known as the "right to be forgotten": The data subject has the right to delete personal data relating to him or her without undue delay upon his or her request, and the Data Controller is obliged to erase personal data relating to the data subject without undue delay, unless mandatory data management excludes it.

In addition to the above, the Data Controller shall delete the data in accordance with Act CXII. of 2011 and EU Regulation 2016/679 of the European Parliament and the Council, if

- the data processing is unlawful;
- the data is incomplete or incorrect - and this condition cannot be legally remedied - unless deletion is excluded by law;
- the purpose of data management has ceased to exist or the statutory period for storing data has expired;
- it has been ordered by a court or the Authority;
- personal data are no longer needed for the purpose for which they were collected or otherwise processed;
- the data subject objects against the data processing and there is no overriding legitimate reason for the data processing;
- personal data must be deleted in order to comply with a legal obligation under the law applicable to the Data Controller;
- personal data were collected in connection with the provision of information society services directly to children referred to in Article 8 (1) of EU Regulation 2016/679.

In the event that the Data Controller has, for any reason, disclosed personal information and is required to delete it as described above, taking into account the available technology and the costs of implementation it shall take reasonable steps, including technical measures, to inform other data controllers involved into the data management that the data subject has requested the removal of links to, or a copy or duplicate of, that personal data.

The Data Controller draws the attention of the data subject to the limitations of the EU Regulation on the right of deletion or "the right to be forgotten", which are:

- a) the exercise of the right to freedom of expression and information;
- b) fulfilling an obligation under the Union or national law applicable to the Data Controller for the processing of personal data or performing a task in the public interest or in the exercise of official authority vested in the Data Controller;
- c) public interest in the field of public health;
- d) in accordance with Article 89 (1) of EU Regulation 2016/679, the process for archiving in the public interest, for scientific and historical research purposes or for statistical purposes, the right to erasure if applied would be likely to render impossible or seriously compromise these data processings; or

e) the filing, enforcement or defense of legal claims.

Right to restrict or otherwise block the data management: the data subject has the right to restrict the data management upon request.

Where, on the basis of available information, it is considered that deletion would harm the data subject's legitimate interests, data shall be blocked. The blocked personal data may only be processed for as long as the purpose of the data processing, which precludes the deletion of the personal data, is fulfilled.

If the data subject disputes the accuracy or pertinence of the personal data but the inaccuracy or incorrectness of the personal data in question cannot be clearly established, the data shall be blocked. In this case, the restriction applies to the period of time that allows the Data Controller to verify the accuracy of personal data.

EU Regulation requires data to be blocked if

- a) the data processing is unlawful, and the data subject opposes the erasure of the data, and instead requests that their use be restricted;
- b) the Data Controller no longer needs personal data for the purposes of data processing, but the data subject requires them to make, assert or defend a legal claim; or
- c) the data subject has objected to the processing; in this case, the restriction shall apply for a period until it is ascertained whether the legitimate reasons of the Data Controller take precedence over the legitimate reasons of the data subject.

Where processing is subject to a restriction (blocking), such personal data shall only be processed, with the exception of the storage, with the consent of the data subject or for the purpose of claiming, asserting or defending legal claims or for the purpose of protecting rights of other natural or legal persons or for important Union or Member State public interests.

The Data Controller hereby specifically draws the attention of the data subjects to the fact that their right to rectification, erasure or blocking may be restricted by law in the interests of external and internal security of the State, such as national defense, national security, the prevention or prosecution of crime, the security of law enforcement, the economic or financial interests of the State or local authorities, moreover, for the purposes of protecting the economic or financial interests of the European Union, and preventing and detecting disciplinary and ethical misconduct in connection with the exercise of the profession and breaches of labor law and safety, including in all cases monitoring and surveillance, and for the protection of the rights of the data subject or of others.

The Data Controller shall, without undue delay and within a maximum of 30 days of receipt of the request, inform the data subject of its request and / or rectify the data and / or delete and / or restrict (block) the data or take any other action in accordance with the request, unless there is a reason to exclude it.

The Data Controller shall notify the data subject in writing of the rectification, deletion and restriction of data management, as well as those to whom the data have previously been transmitted for data management purposes. At the request of the data subject, the Data Controller shall inform those recipients. Notification may be dispensed with if the purpose of the processing does not adversely affect the legitimate interest of the data subject, or if the information proves impossible or involves a disproportionate effort. The Data Controller shall also inform the data subject in writing if the data subject is not able to exercise his / her rights for any reason and shall state precisely the factual and legal reason and the remedies open to him / her: access to court and to the National Data Protection and Freedom of Information.

The "right to data portability": The data subject is entitled to

- a) receive personal data relating to him or her which he or she has made available to the Data Controller in a structured, widely used, machine-readable format and has the right to:
- b) transfer this data on to another data controller

without the obstruction of the data controller to whom the personal data have been made available, provided that:

- a) the data management is based on consent;
- b) the data are processed in an automated way.

In exercising his right to data portability, the data subject shall have the right, where technically possible, to request the direct transfer of personal data between data controllers.

In view of the data management performed by the Data Controller, the conditions for exercising data portability rights are not fulfilled (there is no automated data management) and therefore the data subject cannot exercise this right.

Right to object: The data subject may object to the processing of their personal data, including profiling, if

- the processing (transfer) of personal data is necessary only for the enforcement of the rights or legitimate interests of the Data Controller or the data recipient, except in case of mandatory data processing;
- the use or transfer of personal data for the purpose of direct marketing, opinion polling or scientific research;
- the exercise of the right to object is otherwise permitted by law.

The data subject may even object under Article 21 (3) of EU Regulation 2016/679. the purposes of direct marketing, in this case the personal data shall no longer be processed for that purpose.

Where personal data are processed for scientific and historical research or statistical purposes, the data subject shall have the right to object to the processing of personal data relating to him or her for reasons relating to his or her situation, unless necessary for the performance of a task carried out in the public interest.

The Data Controller shall, with the simultaneous suspension of the data processing, examine the objection as soon as possible after filing the application, but within a maximum of 30 days, and shall inform the applicant in writing of the result. If the applicant's objection is well founded, the Data Controller shall terminate the data processing, including further data collection and transfer, and shall block the data and inform anyone to whom the personal data subject to the objection have previously been transmitted of the objection and who are required to take action to enforce the right to object.

If the data subject disagrees with the decision of the Data Controller or if the Data Controller fails to comply with the time limit referred to above, he or she shall have the right to go to law within 30 days of its notification.

The data subject has the right to object to automated decision making.

Judicial Enforcement: The data subject can go to court if his or her rights are violated. The court will deal with the matter out of turn. The Data Controller shall prove that the data management complies with the provisions of the law.

In case of violation of right to self-determination, a complaint or notice may be filed to: National

Authority for Data Protection and Freedom of Information  
Address: H-1125 Budapest, Szilágyi Erzsébet fasor 22/c  
Phone: +36 (1) 391-1400, Fax: +36 (1) 391-1410  
www: <http://www.naih.hu>  
e-mail: [ugyfelszolgalat@naih.hu](mailto:ugyfelszolgalat@naih.hu)