

PRIVACY POLICY

for Guests

In the course of operating the Hotel located at Balatonföldvár, Báthory István u. 40., the Trade Union of Teachers as an accommodation service provider (hereinafter the “Controller”) manages the data of persons using the accommodation services and of those travelling with them (hereinafter “Guest” and “Data Subject”) in order to provide appropriate services to them. In this document, the Trade Union of Teachers informs Data Subjects about the personal data it controls, the purposes of and legal basis for data processing, the data processing practices applied, and about how Data Subjects can exercise their rights.

The Controller consents to be bound by this legal document that concerns data management it performs in the framework of its activities. The Controller reserves the right to modify this Privacy Policy (hereinafter the “Policy”).

1. Legislation for data management

- Regulation (EU) 2016/679 of the European Parliament and 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 (hereinafter the “GDPR” or the “Regulation”);
- Act CXII of 2011 on the right of informational self-determination and on freedom of information (hereinafter the “Info Act”);
- Act of 2013 on the Civil Code (hereinafter the “Ptk”);
- Act CLVI of 2016 on the state’s responsibilities regarding the development of tourism regions (hereinafter the “Tourism Act”);
- Government Decree 235/2019. (X.15.) on the implementation of Act CLVI of 2016 on the state’s responsibilities regarding the development of tourism regions;
- Government Decree 239/2009 (X.20.) on the detailed conditions for engagement in accommodation service activities and the procedure for the issuance of accommodation licences.

2. Name and contact details of the accommodation service provider / Controller:

Name of Controller: Trade Union of Teachers, Head Office

Reg. nr. of Controller: 01-02-0000200

Tax nr. of Controller: 19002347-2-42

Seat of Controller: 1068 Budapest, Városligeti fasor 10.

Representative: Éva Zsuzsanna Szabó, President

Data Protection Officer: Dr. Bernadett Krizsán

Phone number of Controller: +36-1- 322-8452

3. Definitions

Regarding the concepts used in this Policy, the definitions specified in Art. 4 of the GDPR apply, in accordance with the interpretative provisions of the Tourism Act and of the Decree on its implementation. The definitions are as follows:

- **“Personal data”**: Any information relating to an identified or identifiable natural person (“Data Subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- **“Data Subject”**: An identified or identifiable natural person. In the context of this document, it primarily refers to Guests.
- **“Consent”**: Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
- **“Controller”**: The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
- **“Processing”**: 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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- **“Processor”**: A natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller;
- **“Accommodation facility”**: as defined in Act CLXIV of 2005 on trade (hereinafter the “Trade Act”);
- **“Accommodation service provider”**: A business organisation (a company, a private individual with tax nr. relating to their activities, or a private entrepreneur) providing services specified in Art. 23 and 24 of the Trade Act;
- **“Personal identifying information”**: A person’s a) first and last name, b) place of birth, c) date of birth, and d) mother’ maiden name.
- **“Accommodation facility management software”**: A computer application that must be used by the accommodation service provider, which is connected to a document scanner and is able to transfer stored data to the National Tourism Data Supply Centre (NTDSC) and to a server space, and any computer application specified in Art 9/I. § (2) of the Tourism Act;
- **“Guest”**: A natural person who actually uses accommodation services and stays at the accommodation facility, regardless of who pays for the accommodation services;
- **“Guest data”**: Personal data stored by the tourism hosting service provider as the processor of the accommodation service provider relating to guests as specified in Art. 9/H. § (1) of the Tourism Act.

4. Description of data processing activities

The accommodation service provider as Controller records the personal data specified in this paragraph on a dedicated server space maintained by the Hungarian Tourism Agency (hereinafter “HTA” or the “tourism hosting service provider”).

The IT system of NTDSC collects data for national statistical purposes and is operated by HTA. NTAK stores data that contains no personal information and falls into the scope of statistical data, transmitted by accommodation service providers using the accommodation facility management software.

<p>Scope of processed data</p>	<p><u>Mandatory data:</u></p> <ul style="list-style-type: none"> • Guest’s name (and name at birth), place and date of birth, sex, nationality, mother’s maiden name; • Identification data of the Guest’s document suitable for personal identification and/or travel document (nr. of visa or residence permit, date and place of entering the country); • Time of checking in and of expected and actual checking out. • Guests are required to show their documents for data recording purposes (without making photocopies). <p><u>Optional data</u> (Guests can provide this data voluntarily): permanent address, email address, phone number, TUT membership number.</p>
<p>Purpose of data processing</p>	<p>When a Guest checks in, in order to ensure the protection of the rights, safety and property of Guest and other persons, the accommodation service provider as Controller records his/her data on the server space maintained by the hosting service provider via the accommodation facility management software.</p> <p>Optional data is recorded for contact purposes.</p>
<p>Legal basis for data processing</p>	<p>The legal basis for processing mandatory data is to comply with the legal requirements specified in Art. 6 (1) c) of the GDPR and Art. 9/H. of the Tourism Act; the legal basis for processing optional data is to obtain consent as per Art. 6. (1) a) of the GDPR; and in the case of special personal data Art. 9. (2) a) of the GDPR.</p>
<p>Duration of storing data</p>	<p>The accommodation service provider stores the collected personal data until the last day of the year following the year of data collection.</p>
<p>Method of storing data</p>	<p>Electronic files (on the HTA server via the accommodation facility management software) and hard copies.</p>
<p>Data source</p>	<p>Data Subject</p>
<p>Potential consequences if data provision does not take place</p>	<p>If data provision does not take place, the Controller cannot provide the accommodation service requested by the Data Subject. If the Data Subject fails to show his/her document(s), the Controller rejects the request for accommodation service.</p>
<p>Who will have access to personal data?</p>	<p>The authorised employees of the Controller have access to the data provided by the Guest. In line with the relevant provisions, the Controller enters the personal data into the IT system specified by the relevant legal provisions.</p>
<p>Transmission of data to third countries or to international organisations</p>	<p>No data shall be transmitted to third countries or to international organisations.</p>

5. Processor

As hosting service provider and Processor of the accommodation service provider, HTA is responsible exclusively for storing the data on the guest data server encrypted using the method specified by the relevant government decree, and for providing access to the data for the person or authority specified by the accommodation service provider in accordance with the relevant provisions. The hosting service provider shall have no access to the data stored on the server.

The server accepts data packages only if the sender has encrypted the data content to be protected using the encryption key defined in the relevant legal provision. The key service provider responsible for data encryption is the MPF Felügyeleti Szolgáltató Kft.

6. Data transmission

- 6. 1.** The Controller stores data provided by the Guest in accordance with the purpose of storing the specific data.
- 6. 2.** At special authority requests and at the request of official entities authorised by law, the Controller shall provide information, transmit data, and make specific documents available. If the authority requesting data has specified the reason for its request and the scope of data, the Controller may release personal data only to the extent it is justified by the reason for the request.
- 6. 3.** For the purposes of criminal investigations, crime prevention, and in order to maintain public order, public safety and border control, and to protect the rights, safety and property of Data Subjects and other persons, and to execute a warrant of caption, the police
 - may search the data stored on the server of the hosting server provider using IT devices, and based on the search results they are allowed to identify the accommodation service provider where the person who fulfils the search criteria is registered as a service user, and
 - may request the transmission of the data managed by the hosting service provider after specifying the reason for their request for data.
- 6. 4.** The Controller shall transmit data that includes no personal information and falls into the scope of statistical data to the National Tourism Data Supply Centre. THA, which operates NTDSC, is entitled to use the data provided by the accommodation service provider for research and development in order to develop tourism, and to prepare and publish summaries, status reports, evaluations and forecasts, without disclosing any data suitable for personal identification.
- 6. 5.** The annual data provision to the competent notary shall contain no personal data.

7. Data security

In the framework of its operations, the accommodation service provider as Controller is responsible for the storage and secure management of the collected data, for the protection of non-public data, and for fulfilling its obligations regarding the protection of secrets.

Guest data is stored in encrypted form in the IT system operated by the tourism hosting service provider: The tourism hosting service provider, based on the available technologies and the nature and purpose of data management, and considering the risks to the rights and freedoms of natural persons, shall implement appropriate technical and organisational measures in order to ensure the appropriate level of security, depending on risk level, by encryption, and ensures that its employees have no access to guest data.

For details regarding the accommodation facility management software and the secure operation of NTDSC, see THA's (Operator) Acceptable Use Policy.

8. The rights of Data Subjects

8.1. The right to access

The Data Subject is entitled to receive information from the Controller regarding whether their personal data is managed, and if it is, they are entitled to access the personal data and other information specified in the Regulation.

8.2. The right to rectification

The Data Subject may request the Controller to rectify inaccurate personal data about the Data Subject without unreasonable delay. Depending on the purpose of data collection, the Data Subject may request the addition of missing personal information.

8.3. The right to erasure

In specific cases set out in the Regulation, the Data Subject may request the Controller to erase the personal data managed by the Controller based on the consent of the Data Subject without unreasonable delay.

8.4. The right to be forgotten

If the Controller is required to erase personal data it disclosed earlier, the Controller shall make all reasonable efforts, including taking the necessary technical measures, to notify controllers handling the data that the Data Subject has requested the erasure of links to and the copies and duplicates of the personal data in question, also taking the available technology and the related costs into consideration.

8.5. The right to the restriction of processing

The Data Subject may request the Controller to restrict data processing if the conditions specified in Art. 18. (1) of the GDPR are fulfilled.

8.6. The right to portability

The Data Subject may request the Controller to deliver his/her personal data to him/her, and is entitled to transmit those data to another controller.

8. 7. The right to object

The Data Subject may object to the management of their personal data any time.

Request for information

The Data Subject is entitled to request information from the Controller regarding the processing of the Data Subject's personal data. The Data Subject may execute his/her right to access, to erasure, to rectification, to the restriction of processing, to portability, and to object to data processing through the following channels:

- Postal mail: 1068 Budapest, Városligeti fasor 10.
- Email: psz@pedagogusok.hu

Deadline for fulfilling requests

The Controller shall inform the Data Subject in writing about the measures taken regarding the said requests without unreasonable delay, but within no more than 30 days of the date of receiving the request.

The period specified above can be extended by 30 days in justified cases. The Controller shall notify the Data Subject about the extension of the deadline and the reason for the delay within 30 days of the date of receiving the request.

If the Controller takes no measures in response to the Data Subject's request, it shall, without unreasonable delay but within 30 days of the date of receiving the request, notify the Data Subject about the factual and legal basis for rejecting the request, the reasons for not taking any measures, and that the Data Subject is entitled to submit a complaint to the supervisory authority specified in Point XV., or can execute his/her right to legal remedies.

9. Notifying the Data Subject about a data protection incident

The Controller shall notify the Data Subject in a clear and easy-to-understand manner about any data protection incident without unreasonable delay, if the incident is likely to involve high risk to the rights and freedoms of the Data Subject(s).

In the notification the Controller is required to describe the nature of the data protection incident, to specify the name and contact details of the person who can provide further information, to explain the likely consequences of the data protection incident, and to explain the measures taken or planned in relation to the incident, including measures to mitigate the potential negative consequences of the incident.

The Controller is exempt from the obligation to notify users in the cases specified by Art. 34. (3) of the GDPR.

10. Available legal remedies

10. 1. The Data Subject may contact the Controller to indicate his/her remarks regarding the processing of his/her personal data via the contact details specified in Point 2.

If following complaint management the Data Subject is still not satisfied with the way his/her data is managed by the Controller, or would like to turn directly to the competent authority, (s)he can submit a complaint to the Hungarian National Authority for Data Protection and Freedom of Information (address: 1055 Budapest, Falk Miksa utca 9-11.; mailing address: 1363 Budapest, Pf.: 9. Email: ugyfelszolgalat@naih.hu; website: www.naih.hu).

- 10. 2.** If the Data Subject thinks that his/her rights have been violated, (s)he can take legal action against the Controller. The court shall handle such complaints with priority.
- 10. 3.** If the Data Subject provided data of a third party in order to use the services or caused damage in any way to the Controller, the Controller may claim damages. In such cases the Controller shall do everything in its capacity to assist the competent authorities to identify the offender.

11. Other provisions

Only the Head Office of the Trade Union of Teachers has a right to use this Privacy Policy.

This document remains in force from 1 April 2021 until withdrawal.
