



THERMAL HOTEL VISEGRÁD
★★★★ SUPERIOR

PRIVACY POLICY

**THERMAL HOTEL VISEGRÁD Kereskedelmi és Szolgáltató Zártkörűen Működő
Részvénytársaság**

For Guests

25/05/2018

Table of Contents

I. General provisions and the Controller's contact information	2
II. Processing the data of clients, partners, and shareholders	3
II.1. The legal basis for data processing	3
II.2. The purpose of data processing	3
II.3. The term of data processing	4
II.4. The range of processed data.....	4
II.5. Statement on the use of IT support	4
II.6. Persons entitled to access the data	5
III. Security cameras	5
III.1. The legal basis for data processing	5
III.2. The purpose of data processing	5
III.3. The term of data processing	6
III. 4. The range of processed data.....	6
III.5. Statement on the use of IT support	6
III.6. Persons entitled to access the data	6
IV. The rights of data subjects regarding data processing.....	7
IV.1. Information	7
IV.2. Rectification of data.....	8
IV.3. Erasure and blocking of data	9
IV.4. Objection to the processing of personal data.....	9
v. Remedies available to the data subject	10

I. General provisions and the Controller's contact information

The purpose of the Privacy Policy is to ensure that data subjects receive suitable information on rights and obligations in connection with the processing of their personal data. With the use of this Policy, data subjects can learn of the circumstances of the processing of their personal data, allowing them to make well-founded decisions on granting their consent to the same.

This Privacy Policy is based on Section 20 (2) of the Information Act, which states that, before processing operations are carried out, the data subject shall be clearly informed in detail of all aspects concerning the processing of their personal data, such as the purpose for which the data is required and the legal basis, the person entitled to control the data and to carry out the processing, the duration of the proposed processing operation, if the data subject's personal data is processed in accordance with Section 6 (5) of the Information Act, and the persons to whom his data may be disclosed. Information shall also be provided on the data subject's rights and remedies.

Under Section 4 (1) of the Information Act, personal data may only be processed for specified and explicit purposes, where it is necessary to exercise certain rights and fulfil obligations. The purpose of processing must be satisfied in all stages of data processing operations; recording of personal data shall be under the principle of lawfulness and fairness. Under Section 4 (2) of the Information Act, the personal data processed must be essential for the purpose for which it was recorded, and it must be suitable for achieving that purpose. Personal data may be processed to the extent and for the duration necessary to achieve its purpose.

This Privacy Policy pertains to the personal data that THERMAL HOTEL VISEGRÁD Kereskedelmi és Szolgáltató Zártkörűen Működő Részvénytársaság collects and processes in connection with its clients, employees, shareholders, and partners (hereinafter: data subjects).

By way of this Privacy Policy, THERMAL HOTEL VISEGRÁD Kereskedelmi és Szolgáltató Zártkörűen Működő Részvénytársaság informs data subjects of the facts pertaining to data processing prior to starting processing. The information set out in the Privacy Policy extends to the rights of and remedies available to data subjects in connection with data processing and whether a processor is used in the course of data processing.

For the purposes of all data processing specified in the Privacy Policy, THERMAL HOTEL VISEGRÁD Zrt. is the Controller.

The data and contact information of the Controller

- **THERMAL HOTEL VISEGRÁD Kereskedelmi és Szolgáltató Zártkörűen Működő Részvénytársaság**
- Registered seat: 2025 Visegrád, Lepence völgy 2.
- Commercial register code: 13-10-040734
- Tax number: 12565317-2-13
- Represented by: Gábor Nádas, General Manager

Relevant contact information:

- **THERMAL HOTEL VISEGRÁD Zrt.**
- Address: 2025 Visegrád, Lepence völgy 2.
- Tel.: +36 26-801-900
- Email: horvathr@thv.hu
- Controller's website: <http://www.thv.hu>

The Privacy Policy is available online at the website <http://www.thv.hu>, under the Privacy Policy menu item.

II. Processing the data of clients, partners, and shareholders

THERMAL HOTEL VISEGRÁD Zrt. (hereinafter: Company) processes the personal data of the natural persons of its clients, partners, and shareholders in connection with its own activity based on its own data protection and processing rules, to be interpreted together with this Privacy Policy.

II.1. The legal basis for data processing

The voluntary consent of the data subject given when the data subject sends a request for a quotation or any other contact concerning any business affairs to THERMAL HOTEL VISEGRÁD Zrt. [Section 5 (1) (a) of the Information Act] or if such is necessary for the role of shareholder in the Company.

II.2. The purpose of data processing

THERMAL HOTEL VISEGRÁD Zrt. processes the personal data included in the documents that it has received either directly or indirectly for the purposes of its own core activity and providing the services necessary for its operations, especially in the interest of promoting business with its own contractual partners and business partners and to be able to perform such activities smoothly and to appropriate quality.

The Company also processes personal data for the purposes of keeping records of the entitlements of the shareholders and to ensure that such entitlements are provided in

accordance with relevant legislation.

II.3. The term of data processing

The personal data of data subjects is processed in connection with the performance of the contract pertaining to the services specified in point II.2 and, based on the consent of data subjects, the personal data of the given natural person is retained for the specific purpose for 8 years following the achieving of the purpose of processing.

In accordance with the purpose specified in point II.2 and the activities of the Controller Company, and in line with the interests of the data subjects, data processing shall take place for 8 years following the achieving of the purpose of processing. Retention for this term shall be interrupted by any request for erasure submitted by the data subject, in which case the Controller shall immediately erase the personal data of the given data subject from the database.

In line with Section 6 (5) (a) of the Information Act, if the Company is required to process the data due to a legal obligation, the Company shall process the data for the term of such obligation.

Applicants may request the erasure of their data and may withdraw the consent they have given by writing to the address 2025 Visegrád, Lepence völgy 2. or to horvathr@thv.hu.

II.4. The range of processed data

First name, surname, sex, date of birth, email address, telephone number, and all other data/information voluntarily disclosed by the data subject

II.5. Statement on the use of IT support

As hosting service providers contracted by the Controller, the following companies provide the technical conditions necessary for digital data storage:

Nethotelbooking Kft.

Registered seat: 8200 Veszprém, Boksa tér 1/A

Represented by: Zsuzsa Szilágyi

Aramor Kft.

Registered seat: 1041 Budapest, Závodszky u.

39.

Represented by: Balázs Lerner

MT-Hostware Kft.

**Registered seat: 1149 Budapest, Róna u. 120-
122.**

Represented by: György Lehel

Creative Management Kft.

**Registered seat: 8200 Veszprém, Boksa tér 1.
Building A**

Represented by: Zoltán Gál

Soto Trade Kft.

**Registered seat: 1081 Budapest, II. János Pál pápa
tér 11.**

Represented by: Attila Toró

Árgus-Security Kft.

**Registered seat: 1024 Budapest, Lövőház utca
9.**

Represented by: György László

[II.6. Persons entitled to access the data](#)

THERMAL HOTEL VISEGRÁD Zrt only uses the data for the purposes of exercising its own activities. We declare that the persons employed or otherwise contracted by the company can only access the personal data of data subjects for the purposes of data processing.

III. Security cameras

THERMAL HOTEL VISEGRÁD Zrt. (hereinafter: Company), as employer and Controller, based on its own data protection and processing rules, to be interpreted together with this Privacy Policy, operates an electronic surveillance system suitable for recording images, audio, and video. Annex M.1, attached hereto, contains the current state of the Company's video system, which data subjects may request from the Controller for information purposes, in the manner specified in point V.1.

III.1. The legal basis for data processing

With the consent of the data subjects, recordings are processed in line with the Company's lawful interests.

III.2. The purpose of data processing

THERMAL HOTEL VISEGRÁD Zrt. only makes security recordings using its electronic surveillance system for the purposes of property protection and security technology.

III.3. The term of data processing

Personal data is always processed by taking into account the time limit under Section 31 (2) and (3) of Act CXXXIII of 2005 on Personal and Property Security and Private Investigation Activities.

In line with Section 6 (5) (a) of the Information Act, if the Company is required to process the data due to a legal obligation, the Company shall process the data for the term of such obligation.

III.4. The range of processed data

Image recording.

III.5. Statement on the use of IT support

As a data processor contracted by the Controller, the following company provides the technical conditions necessary for digital data storage:

Soto Trade Kft.

Registered seat: 1081 Budapest, II. János Pál pápa tér 11.

Represented by: Attila Toró

Árgus-Security Kft.

Registered seat: 1024 Budapest, Lövház utca 9.

Represented by: György László

III.6. Persons entitled to access the data

The company only processes the data in the interest of the lawful implementation of property

protection and security technology purposes, in connection with which the company's general manager and the employees employed by the company have access to the personal data specified in this point.

IV. The rights of data subjects regarding data processing

Rights of the data subject:

- request for information
- request for rectification of data
- request for the erasure or blocking of data
- object to data processing

Requests concerning information, rectification, blocking, erasure, and objections pertaining to the personal data may be notified at any time at the following points of contact:

- by mail: 2025 Visegrád, Lepence völgy 2.
- by email: igazgatosag@thv.hu,
- by telephone: +36 26-801-900, by providing their name and address,
- in person: 2025 Visegrád, Lepence völgy 2.

IV.1. Information

The data subject (hereinafter: user) may request THERMAL HOTEL VISEGRÁD Zrt. (hereinafter: Controller) to provide information on the processing of personal data at any time. The Controller must comply with requests for information without any delay, and provide the information requested in an intelligible form, in writing at the data subject's request, within no more than 25 days.

The User may submit requests for information to the Controller by mail, fax, or email. In the request, the User is required to indicate identification data based on which the Controller can determine the User's eligibility to access the personal data in question. In the request, the User is required to provide electronic contact information or a correspondence address to which the Controller can send the requested information.

The User may request information on the range of processed data, the source of the personal data, the purpose of the processing of personal data, the legal basis for processing by the Controller, the term of processing by the Controller, and the Controller's activities related to the processing of personal data.

In case of a request to such effect, the Controller shall provide information on the contractual

partners to which it has transferred personal data and the legal basis for the data transfer.

Should any data security breach occur in the course of processing, the User may request information on the circumstances and effects thereof as well as the measures taken by the Controller to mitigate the same. A data security breach means that processing or handling of personal data takes place in a manner that is in violation of the law. This especially applies if an unauthorised person gains access to personal data, if personal data are unlawfully amended, transferred, or published, or if personal data are unlawfully erased or destroyed. A data security breach shall also have occurred if the personal data is destroyed or damaged as the result of an accident.

The Controller shall provide the requested information by email within 25 days of receipt of the User's request. If the User submitting the request has not provided an email address in the request or specifically requests the information to be posted, the Controller shall post the information in written form. The Controller shall provide such information to the range of persons specified in the personal data request free of charge on one occasion per year.

The Controller may refuse to provide information to the data subject in the following cases:

- If, in the case of data transfer, the Controller receives the personal data from the data transferor after the data transferor has informed the Controller that the data subject's right to information is restricted by any Hungarian or international laws.
- If the rights of the data subject to information are restricted by law in order to safeguard the external and internal security of the State (such as defence, national security, the prevention and prosecution of criminal offences, or the safety of penal institutions), to protect the economic and financial interests of central and local government, to safeguard the important economic and financial interests of the European Union, to guard against disciplinary and ethical breaches in regulated professions, to prevent and detect breaches of obligation related to labour law and occupational safety (including in all cases control and supervision), and to protect data subjects or the rights and freedoms of others.

Even if the information is refused under this point, the Controller shall inform the data subject in writing of the reason for refusal, as well as indicating the exact legal basis. In this case, the Controller shall also inform the data subject of the possibilities for seeking judicial remedy or lodging a complaint with the Authority (in regard to remedy, please see point IV of this Policy below).

[IV.2. Rectification of data](#)

The data subject may call upon the Controller at any time to rectify its data if they are incorrect.

If the personal data are false or erroneous and the Controller has the genuine or correct personal information at its disposal, the Controller will rectify the personal data. The data subject may submit requests for the rectification of information to the Controller by mail or email.

If the Controller refuses to comply with the data subject's request for rectification within 25 days of receipt of the request, it shall notify the data subject in writing or, with the consent of the data subject, by email of the reasons for refusal and the legal basis of the same. In this case, the Controller shall also inform the data subject of the possibilities for seeking judicial remedy or lodging a complaint with the Authority.

IV.3. Erasure and blocking of data

The data subject may call upon the Controller to erase or block its personal data at any time. The data subject may send the request for erasure or blocking to the Controller by mail or email.

The Controller shall erase personal data if:

- it had been processed unlawfully,
- the data subject requested erasure or blocking of its personal data,
- the data processing is incomplete or inaccurate and it cannot be lawfully rectified, provided that erasure is not disallowed by law,
- the purpose of processing no longer exists or the legal time limit for storage has expired,
- the erasure of the data has been ordered by a court or the Authority.

If the Controller refuses to comply with the data subject's request for erasure or blocking within 25 days of receipt of the request, it shall notify the data subject in writing or, with the consent of the data subject, by email of the reasons for refusal and the legal basis of the same. In this case, the Controller shall also inform the data subject of the possibilities for seeking judicial remedy or lodging a complaint with the Authority.

Personal data shall be blocked instead of erased if so requested by the data subject, or if there are reasonable grounds to believe that erasure could affect the legitimate interests of the data subject. Blocked data shall only be processed for the duration of the legislative or factual circumstance which prevented their erasure.

IV.4. Objection to the processing of personal data

The data subject may object to the processing of personal data pertaining to themselves in the following cases:

- if the processing of personal data is only necessary for

the fulfilment of the Controller's legal obligations or to validate the vital interests of a third person,

- if the purpose of the processing of personal data is direct marketing, public opinion polling, or scientific research,
- if the data subject is permitted to do so by law.

The data subject may submit its objection to the Controller by mail or email. The Controller shall examine the objection and decide on whether it is sound within 15 days of submission. The Controller shall inform the data subject of its decision in writing. If the data subject's objection is justified, the Controller shall terminate all processing operations (including data transmission), block the data involved, and notify all recipients to whom any of the personal data had previously been transferred concerning the objection and the ensuing measures, upon which these recipients shall also take measures regarding enforcement of the objection.

V. Remedies available to the data subject

If the data subject does not agree with the Controller's decisions or if the Controller fails to comply with the 15-day deadline available to assess the data subject's objection, the data subject may, within 30 days of the notification of the decision of the last day of the time limit, turn to a court to seek remedy.

The data subject may turn to the National Authority for Data Protection and Freedom of Information if their rights have been violated in connection with the processing of personal data, or it may also initiate legal proceedings at the competent court.

The National Authority for Data Protection and Freedom of Information can be contacted at the following:

- Address: 1125 Budapest, Szilágyi Erzsébet fasor 22/c
- Postal address: 1530 Budapest, Pf.: 5.
- Telephone: +36 (1) 391-1400
- Fax: +36 1- 391- 1410
- Email: ugyfelszolgalat@naih.hu
- Website: www.naih.hu

The data subject may bring the action against the Controller before the tribunal in whose jurisdiction the data subject's home address or temporary residence is located.

The data subject is only entitled to consent to data processing by the Controller if they have

understood the above data protection and data processing provisions and are aware of their rights and obligations in connection with data processing.

Visegrád, 25 May 2018

THERMAL HOTEL VISEGRÁD Zrt.

Represented by: Gábor Nádas

General Manager