Privacy Policy

Lombard Gold Zrt. (1196 Budapest, Ady Edre st. 97-99. 3 ép. E. house. 4. door

NN Boutique Hotel

(3580 Tiszaújváros, Tiszavirág street 18.)

Table of Contents

Contents

Table of Contents 2
I. PREAMBLE: 4
I.1. Purpose of Establishing the Policy 4
II. Temporal, Subject, and Personal Scope of the Policy: 6
II.1. Definitions: 6
"personal data": 6
"data processing": 6
"restriction of data processing": 6
"data controller": 6
"data processor": 6
"recipient": 6
"third party": 6
"consent of the data subject": 7
"data protection incident": 7
"enterprise": 7
III. Basic Rules of Data Processing: 7
IV. Principles of Data Protection: 8
IV.1. Lawfulness of Data Processing: 8
IV.2. Conditions of Consent: 9
V. The Company's Data Protection System 9
V.1. Responsibilities of the Managing Director Regarding Data Protection: 10
V.2. Data Security Rules for Paper-Based Data Processing: 11
V.3. Data Security Rules for Electronic Data Processing: 12
V.5. Reporting a Data Protection Incident to the Supervisory Authority: 12
V.6. Informing the Data Subject About the Data Protection Incident: 13
VI. Rights of Data Subjects: 14
VI.1. Transparent Information, Communication, and Measures to Facilitate the Exercise of Data Subject Rights 14
VI.2. Right of Access of the Data Subject: 15
VI.3. Right to Rectification: 16
VI.4. Right to Erasure ("Right to be Forgotten"): 16
VI.5. Right to Restriction of Processing: 17
VI.6. Notification Obligations Related to Rectification, Erasure, or Restriction of Data Processing: 17
VI.7. Right to Data Portability: 17
VI.8. Right to Object: 17
VII. Rules on Complaints, Legal Remedies, and Compensation: 18
VII.1. Right to Lodge a Complaint with the Supervisory Authority: 18
VII.2. Right to Effective Judicial Remedy Against the Supervisory Authority: 19
VII.3. Right to Effective Judicial Remedy Against the Data Controller or Processor: 19
VII.4. Right to Compensation and Liability: 19
VII.5. Representation in Remedies and Court Proceedings: 20
VIII. Processing of Special Categories of Personal Data: 20
IX. Transfer of Data Abroad (Outside the EU): 21
SPECIFIC DATA PROCESSING ACTIVITIES OF THE COMPANY 22
REQUEST FOR QUOTATION 23
BOOKING 24
CHECK-IN 25
DATA PROCESSING RELATED TO HANDLING CONSUMER COMPLAINTS 26

ELECTRONIC SURVEILLANCE SYSTEM 27
MARKETING PRESENCE ON SOCIAL MEDIA AND COMPANY WEBSITE 29

I. PREAMBLE:

Lombard Gold Private Limited Company (hereinafter: the Company) establishes the following Data Protection Policy (hereinafter: the Policy) to ensure the transparent regulation of its data processing activities, the broad application of data protection principles, as well as the provision of information to data subjects affected by specific data processing activities and the facilitation of the exercise of their rights.

Data Controller Name: Lombard Gold Zrt.
Registering Court: Budapest Metropolitan Court of Registration
Company Registration Number: 01-10142323
Tax Number: 32261754-2-43
Registered Office: 1196 Budapest, Ady Endre út 97-99, Building 3, Entrance E, Ground Floor, Door 4
Branch Office: 3580 Tiszaújváros, Tiszavirág Street 18
Contact Information: nnhotelmail@gmail.com
Representative of the Data Controller: Mihály Kukucska, CEO

The provisions of this Policy shall be interpreted in accordance with the Company's other internal regulations. However, if there is any conflict between the handling or protection of personal data under this Policy and any other regulation adopted before or after the entry into force of this Policy, the provisions of this Policy shall prevail.

I.1. Purpose of Establishing the Policy

From 25 May 2018, the European Union's General Data Protection Regulation (GDPR), adopted by the European Parliament and the Council in 2016 (Regulation (EU) 2016/679), is applicable in Hungary.

The GDPR establishes that the protection of natural persons in relation to the processing of their personal data is a fundamental right, and everyone has the right to the protection of their personal data. Uniform principles and rules concerning the protection of personal data guarantee that the fundamental rights and freedoms of natural persons, especially their right to the protection of personal data, are respected regardless of nationality or residence, and that the privacy of individuals receives adequate protection.

The purpose of this Data Protection Policy is to ensure that the Company, as a data controller, transparently regulates the parts of its activities that qualify as data processing under the GDPR.

This Policy specifies:

- **Which natural persons'**
- **Which personal data**
- **For which specific purposes**
- **On what legal basis**
- **For what duration**
- **According to which principles**
  the Company processes data, and which organizational and technological measures ensure the security of data processing operations, processes, and the personal data managed by the Company.

The Data Controller hereby declares its commitment to protecting the personal data of its natural person clients, partners, and employees, and fully respects the right to the protection of personal data. Accordingly, personal data are processed lawfully in compliance with data protection rules, and all security, technical, and organizational measures are implemented to guarantee data security throughout the processing lifecycle.

The Data Controller acknowledges that it is bound by the contents of this Policy regarding the data processing operations described herein. The Data Controller is obliged to ensure that all data processing activities carried out in connection with its operations are lawful, based on clear and transparent information provided to data subjects, and comply with this Policy, the GDPR, and all applicable national legislation, including but not limited to:

- Regulation (EU) 2016/679 of the European Parliament and of the Council (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, GDPR)
- Act CXII of 2011 on the right of informational self-determination and freedom of information
- Act V of 2013 – Civil Code (Ptk.)
- Act CLV of 1997 – Consumer Protection Act (Fgytv.)
- Act XC of 2017 – Criminal Procedure Code (Be.)
- Act C of 2000 – Accounting Act (Számv. tv.)
- Act CXXXIII of 2005 – Rules on personal and property protection and private investigation activities
- Act XLVIII of 2008 – Restrictions on certain commercial advertising activities (Grt.)
- Act C of 1990 – Local Taxes Act (Htv.)

The Data Controller may modify the content of this Policy at any time, but is obliged to inform data subjects of any changes.

II. Temporal, Subject, and Personal Scope of the Policy:

This Policy remains in effect until its provisions are amended or repealed.

The scope of this Policy extends to all data processing and data handling activities at the Company that involve the personal data of natural persons. Specific data processing activities are precisely defined in this Policy.

All employees of the Company who process or handle personal data in the course of their duties are required to comply with the provisions of this Policy.

II.1. Definitions:

“personal data” – any information relating to an identified or identifiable natural person.

“data processing” – any operation or set of operations performed on personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment, combination, restriction, erasure, or destruction.

“restriction of data processing” – the marking of stored personal data with the aim of limiting their processing in the future.

“data controller” – the natural or legal person, public authority, agency, or other body that alone or jointly with others determines the purposes and means of the processing of personal data.

“data processor” – a natural or legal person, public authority, agency, or other body that processes personal data on behalf of the data controller.

“recipient” – a natural or legal person, public authority, agency, or another body to which personal data are disclosed, whether a third party or not.

“third party” – a natural or legal person, public authority, agency, or body other than the data subject, data controller, data processor, and persons who, under the direct authority of the data controller or data processor, are authorized to process personal data.

“consent of the data subject” – 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.

“data protection incident” – any confirmed or suspected breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored, or otherwise processed.

“enterprise” – any natural or legal person engaged in an economic activity, regardless of the legal form of the activity.

III. Basic Rules of Data Processing:

The processing of personal data by the Company shall comply with the following fundamental rules:

1. **Lawfulness, Fairness, and Transparency:**
   Personal data must be processed lawfully, fairly, and in a transparent manner in relation to the data subject.
2. **Purpose Limitation:**
   Personal data shall be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
3. **Data Minimization:**
   Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
4. **Accuracy:**
   Personal data shall be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that inaccurate personal data are erased or rectified without delay.
5. **Storage Limitation:**
   Personal data shall be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
6. **Integrity and Confidentiality:**
   Personal data shall be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures.

7. **Accountability:**
   The Data Controller is responsible for, and must be able to demonstrate, compliance with the above principles.
8. **Rights of Data Subjects:**
   The Company shall ensure that the rights of data subjects are respected, including access, rectification, erasure, restriction of processing, data portability, and objection rights.

IV. Principles of Data Protection:

Personal data must be:

- **Processed lawfully, fairly, and in a transparent manner** with respect to the data subject ("lawfulness, fairness, and transparency");
- **Collected for specified, explicit, and legitimate purposes** and not further processed in a way incompatible with those purposes ("purpose limitation").

Personal data processed by the Data Controller must also be:

- **Adequate, relevant, and limited to what is necessary** in relation to the purposes for which they are processed ("data minimization");
- **Accurate and, where necessary, kept up to date**; every reasonable step must be taken to ensure that inaccurate personal data are erased or rectified without delay ("accuracy").

The storage of personal data must be in a form that permits identification of data subjects **for no longer than necessary**for the purposes of data processing ("storage limitation"). Furthermore, personal data must be processed in a manner that ensures appropriate security, including protection against **unauthorized or unlawful processing, accidental loss, destruction, or damage** through the use of appropriate technical or organizational measures ("integrity and confidentiality").

The Data Controller is responsible for compliance with these principles and must be able to **demonstrate such compliance** ("accountability").

IV. Principles of Data Protection:

IV.1. Lawfulness of Data Processing:
Personal data shall be processed lawfully. Lawful processing requires that at least one of the following conditions is met:

- The data subject has given consent to the processing of their personal data for one or more specific purposes.
- Processing is necessary for the performance of a contract to which the data subject is a party.
- Processing is necessary for compliance with a legal obligation to which the Data Controller is subject.
- Processing is necessary to protect the vital interests of the data subject or another natural person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.
- Processing is necessary for the legitimate interests pursued by the Data Controller or a third party, except where such interests are overridden by the interests, fundamental rights, or freedoms of the data subject.

IV.2. Conditions for Consent:
Consent must be:

- Freely given: the data subject has a real choice and is not coerced.
- Specific: consent covers clearly defined purposes.
- Informed: the data subject is provided with clear information about the processing.
- Unambiguous: consent is given through a clear affirmative act, such as signing a form, ticking a box, or another active confirmation.

The Data Controller shall be able to demonstrate that the data subject has given consent. The data subject has the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal.

To ensure the above, the data subject may **withdraw their consent to data processing at any time free of charge** by sending a request to the Company's registered office or to **nnhotelmail@gmail.com**. In such cases, all personal data processed based on voluntary consent will be deleted (unless the request concerns only a specific subset of data).

However, certain data may continue to be processed **after withdrawal** in order to comply with **legal obligations** or to pursue **legitimate interests**. Additionally, some data must be processed for a specified period **as required by law** (e.g., retention obligations prescribed by legislation).

V. The Company's Data Protection System

It is the responsibility of the Company's current Managing Director to define the Company's data protection system and, within the framework of this Policy, ensure that the processing of personal data complies with the principles of data processing set forth in this Policy.

All organizational unit heads and employees who process personal data in the course of their duties are responsible for enforcing compliance with the provisions of this Policy.

The Company's data protection system must be designed to ensure optimal security measures so that unauthorized persons cannot access personal data. Personal data, whether in paper or electronic form, must be stored and placed in a manner that allows access only to authorized personnel, and only such personnel may carry out any data processing operations.

Personal data must be protected with appropriate measures, especially against:

- Unauthorized access
- Alteration
- Transmission
- Disclosure
- Deletion or destruction
- Accidental destruction or damage
- Inaccessibility due to changes in the applied technology

The Managing Director is responsible for directing and supervising the Company's data protection system within the framework of this Policy.

V.1. Responsibilities of the Managing Director Regarding Data Protection:

The Managing Director is responsible for:

- Ensuring that data subjects can exercise their rights as defined in this Policy.
- Ensuring the necessary personnel, organizational, and technical conditions for the protection of personal data managed by the Company.
- Addressing any deficiencies or legal violations identified during audits, initiating or conducting procedures to establish personal responsibility.
- Ordering investigations as needed.
- Issuing the Company's data protection regulations.

The Data Controller and Data Processor shall implement appropriate technical and organizational measures, considering the state of science and technology, implementation costs, the nature, scope, circumstances, and purposes of data processing, as well as the varying likelihood and severity of risks to the rights and freedoms of natural persons, to ensure a level of data security appropriate to the risk.

The Company shall ensure, through appropriate measures, that the data of data subjects are available intact for the lawful purpose and duration of processing and that unauthorized access, processing beyond the lawful purpose, disclosure, alteration, or damage/loss of data is prevented.

When determining an appropriate level of security, the Company must consider risks arising from accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to personal data transmitted, stored, or otherwise processed.

It must also be ensured that natural persons under the control of the Data Controller or Data Processor with access to personal data process such data only in accordance with the Company's instructions, unless EU or national law requires otherwise.

Responsibilities of Employees Handling Personal Data:

Employees entrusted with data processing tasks are required to:
a) Fully comply with the provisions of this Policy and sector-specific data protection laws.
b) Inform their direct supervisor, or the Managing Director if necessary, of any data protection issues, opinions, or developments within their responsibilities, including any IT malfunctions, data management problems, or actual or potential data protection incidents.
c) Immediately remedy any irregularities detected in data processing.
d) Perform data backups and ensure secure storage.
e) Provide or transmit data to authorized persons or organizations as required by law.
f) Inform their direct supervisor, or the Managing Director if necessary, if requested or instructed to perform unlawful data processing, and refuse to comply.
g) Immediately report to their direct supervisor any unauthorized access or alteration of data, i.e., any data protection incident.
h) Bear disciplinary and financial responsibility for performing their activities in accordance with the law or, in the absence thereof, in accordance with the consent of the data subject. Non-compliance may result in disciplinary action.

V.2. Data Security Rules for Paper-Based Data Processing:

The Company establishes the following data security rules for paper-based data processing:

- Only authorized personnel may access the data; no one else may view or disclose it.
- Documents must be stored in a securely lockable, dry room equipped with fire protection and property security devices.
- Only authorized personnel may access documents under active use.
- After completing their work, employees handling paper-based data must securely store the documents.
- If paper-based personal data are digitized, the Company shall apply the data security rules applicable to digitally stored documents.

V.3. Data Security Rules for Electronic Data Processing:

For electronic data processing, the Company establishes the following rules:

- Computers used for data processing are the property of the Company, or the Company exercises equivalent ownership rights.
- Access to data on computers is allowed only with valid, personal, identifiable authorization—at least a username and password—and passwords are regularly updated by the Company.
- Continuous antivirus protection is maintained on the network where personal data are processed.
- Available IT tools and systems are used to prevent unauthorized network access.

V.5. Reporting a Data Protection Incident to the Supervisory Authority:

Under this Policy and in accordance with the Regulation, a **data protection incident** is any breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to personal data transmitted, stored, or otherwise processed.

The Company must report a data protection incident to the competent supervisory authority **without undue delay**, and if possible, **within 72 hours** of becoming aware of it, unless the incident is unlikely to result in a risk to the rights and freedoms of natural persons. If reporting within 72 hours is not possible, reasons for the delay must be provided.

The data processor must report the incident to the data controller **without undue delay** upon becoming aware of it.

The report must include at least:

- The nature of the incident, including, if possible, the categories and approximate number of affected data subjects and the categories and approximate number of affected data.
- The name and contact details of a contact person providing further information.
- The likely consequences of the data protection incident.
- Measures taken or planned by the data controller to address the incident, including, where applicable, measures to mitigate potential adverse effects.

The data controller shall maintain a record of data protection incidents, including facts, impacts, and remedial measures, enabling the supervisory authority to verify compliance with these requirements.

V.6. Informing Data Subjects About a Data Protection Incident:

If a data protection incident is likely to result in a **high risk to the rights and freedoms of natural persons**, the affected data subjects must be informed **without undue delay**.

The notification must clearly and understandably describe the nature of the incident and include at least the following:

- Name and contact details of a contact person providing further information.
- Likely consequences of the incident.
- Measures taken or planned by the Company to address the incident, including measures to mitigate any potential adverse effects.

Notification is **not required** if:

- The Company has implemented appropriate technical and organizational protective measures (e.g., encryption) rendering the personal data unintelligible to unauthorized persons; or
- The Company has taken measures after the incident that ensure the high risk to the rights and freedoms of data subjects is unlikely to materialize; or
- Providing notification would require disproportionate effort.

In such cases, data subjects must be informed through publicly available information or similar measures that ensure effective communication.

VI. Rights of Data Subjects

VI.1. Transparent Information, Communication, and Measures to Facilitate the Exercise of Data Subject Rights

The Company shall take appropriate measures to ensure that data subjects receive information regarding the processing of their personal data, as well as all information related to their rights of:

- Access
- Rectification
- Erasure
- Restriction
- Data portability
- Objection

This information shall be provided in a concise, transparent, intelligible, and easily accessible form, using clear and plain language.

Information shall primarily be provided in writing or by other means, including electronically if applicable. Upon explicit request, verbal information may also be provided, provided the identity of the data subject is verified.

The Company is committed to facilitating the exercise of data subject rights (information, access, rectification, erasure, restriction, data portability, objection).

Requests to exercise rights may only be refused if the Company can demonstrate that it is unable to identify the requesting data subject.

Requests must be responded to **without undue delay and at the latest within one month** of receipt, informing the data subject of the measures taken. This period may be extended by an additional two months where necessary, taking into account the complexity of the request and the number of requests, with notification to the data subject. If the request was submitted electronically, the response should also be provided electronically where possible, unless the data subject requests otherwise.

If the Company does not take action, the data subject must be informed without delay, but no later than 30 days after the request, about the reasons for inaction and their right to lodge a complaint with a supervisory authority and to seek judicial remedy.

Information about data subject rights and data protection incidents must be provided free of charge.

If a request is clearly **unfounded or excessive**, particularly due to its repetitive nature, taking into account administrative costs, the Company may:

- Charge a reasonable fee, or
- Refuse to act on the request.

The burden of proving that a request is clearly unfounded or excessive lies with the Company.

Requests may be submitted by post to the Company's registered office, by email to **nnhotelmail@gmail.com**, or verbally, provided that the Company can identify the data subject.

VI.2. Right of Access

Data subjects have the right to obtain confirmation as to whether their personal data are being processed. Where such processing is taking place, they are entitled to access the personal data and the following information:

- The purposes of processing
- The categories of personal data processed concerning the data subject
- The recipients or categories of recipients to whom the personal data have been or will be disclosed, including third-country recipients or international organizations (including necessary safeguards)
- Where possible, the intended retention period of the personal data, or criteria for determining this period
- The right to request rectification, erasure, or restriction of processing, and to object to processing

- The right to lodge a complaint with a supervisory authority
- Where data were not collected from the data subject, all available information about the source

A copy of the personal data being processed shall be provided upon request. For additional copies, the Company may charge a reasonable administrative fee. If the request is made electronically, the information shall be provided in a commonly used electronic format, unless otherwise requested by the data subject.

VI.3. Right to Rectification

Data subjects may request the rectification of inaccurate personal data concerning them **without undue delay and at the latest within one month**. Where processing is based on legal obligations, the data subject must provide proof of the correct data. Considering the purpose of processing, the data subject may also request completion of incomplete personal data, e.g., by providing an additional statement.

The Company reminds data subjects to provide accurate and complete information when sharing personal data, as any consequences arising from incorrect or incomplete information (e.g., incorrectly issued invoices, payments to wrong bank accounts) shall be borne by the data subject, except where rectification is possible without disproportionate effort.

VI.4. Right to Erasure ("Right to be Forgotten")

Data subjects may request the deletion of personal data concerning them **without undue delay and at the latest within one month**, if one of the following applies:

- The personal data are no longer necessary for the purposes for which they were collected or otherwise processed.
- Processing is based on voluntary consent, and the data subject has withdrawn that consent, and there is no other legal basis for processing.
- The data subject objects to processing based on legitimate interests or processing solely for direct marketing purposes, and there is no overriding legitimate reason for processing.
- The personal data have been unlawfully processed.
- Applicable law requires deletion.

Where personal data have been made public, the Company shall, taking into account available technology and implementation costs, take **reasonable steps**, including technical measures, to inform other data controllers of the data subject's request to erase links, copies, or replications of the personal data.

Deletion is not required if processing is necessary, for example, for **the establishment, exercise, or defense of legal claims**.

VI.5. Right to Restriction of Processing

Data subjects have the right to request that the Company **restrict the processing of their personal data** if one of the following applies:

- The data subject contests the accuracy of the personal data; in this case, the restriction applies for the period necessary for the Company to verify the accuracy of the data.
- Processing is unlawful, and the data subject opposes deletion and instead requests restriction of use.
- The Company no longer needs the personal data for the purposes of processing, but the data subject requests their retention for the establishment, exercise, or defense of legal claims.
- The data subject has objected to processing conducted to protect the legitimate interests of a third party; in this case, restriction applies until it is determined whether the controller's legitimate grounds override the data subject's legitimate grounds.

Where processing is restricted, personal data may only be processed **with the data subject's consent**, or for the establishment, exercise, or defense of legal claims, for the protection of another natural or legal person's rights, or for reasons of important public interest of the EU or a Member State, **excluding storage**.

VI.6. Obligation to Notify Third Parties of Rectification, Erasure, or Restriction of Processing

The Company shall inform all recipients to whom personal data have been disclosed of any rectification, erasure, or restriction of processing, unless this proves impossible or involves disproportionate effort. The data subject shall also be informed of such cases.

VI.7. Right to Data Portability

The data subject has the right to receive personal data provided to the Company in a structured, commonly used, and machine-readable format and has the right to transmit those data to another controller if:

- Processing is based on consent or a contract in which the data subject is a party; and
- Processing is carried out by automated means.

Where technically feasible, the data subject may request that personal data be transmitted directly between controllers.

VI.8. Right to Object

The data subject has the right to object **at any time, for reasons related to their particular situation**, to the processing of personal data based on the legitimate interests of the controller. In such cases, the Company shall no longer process the personal data unless it can demonstrate compelling legitimate grounds that override the interests, rights, and freedoms of the data subject, or for the establishment, exercise, or defense of legal claims.

If personal data are processed for direct marketing purposes, the data subject has the right to object at any time to processing of their personal data for such purposes. Personal data may no longer be processed for direct marketing purposes once the objection is made.

VII. Rules on Complaints, Legal Remedies, and Compensation

Data subjects must be informed of their rights to legal remedies and compensation as follows:

VII.1. Right to Lodge a Complaint with the Supervisory Authority

Supervisory Authority: National Authority for Data Protection and Freedom of Information (NAIH)

- Website: https://naih.hu/uegyfelszolgalat,--kapcsolat.html
- Postal Address: 1363 Budapest, Pf.: 9
- Office Address: 1055 Budapest, Falk Miksa u. 9-11
- Phone: +36 (1) 391-1400
- Fax: +36 (1) 391-1410
- Email: ugyfelszolgalat@naih.hu
- URL: http://naih.hu

Without prejudice to other administrative or judicial remedies, the data subject has the right to lodge a complaint with the supervisory authority, particularly in the Member State of their habitual residence, place of work, or the location of the alleged infringement, if they believe that the processing of their personal data violates this Policy or the applicable Regulation.

NAIH guidance on complaint handling: https://naih.hu/panaszuegyintezes-rendje.html

The authority facilitates the enforcement of data subject rights through standard forms, which are available at the above link for the following purposes:

- Requesting information on the processing of personal data
- Requesting rectification of personal data
- Requesting erasure of personal data

VII.2. Right to an Effective Judicial Remedy Against the Supervisory Authority

Without prejudice to other administrative or non-judicial remedies, **every natural and legal person has the right to an effective judicial remedy** against a legally binding decision of the supervisory authority that applies to them.

Furthermore, every data subject has the right to an effective judicial remedy if the competent supervisory authority:

- fails to handle their complaint, or
- does not inform the data subject of the progress or outcome of the complaint within three months.

Proceedings against the supervisory authority shall be brought before the courts of the Member State in which the authority has its seat.

VII.3. Right to an Effective Judicial Remedy Against the Controller or Processor

Without prejudice to available administrative or non-judicial remedies, including the right to lodge a complaint with the supervisory authority, **the data subject has the right to an effective judicial remedy** if they consider that their rights have been infringed as a result of improper processing of their personal data.

Proceedings against the controller or processor shall be brought before the courts of the Member State in which the controller or processor has its place of business. The data subject may also initiate proceedings before the courts of the Member State of their habitual residence.

VII.4. Right to Compensation and Liability

Any person who has suffered **material or non-material damage as a result of a breach of the Regulation** is entitled to compensation from the controller or processor.

All controllers involved in the processing are **liable for any damage caused by unlawful processing**. The processor is liable only if it has **failed to comply with the obligations specifically directed to processors** or has acted contrary to the lawful instructions of the controller.

The controller or processor is **exonerated from liability** if it proves that it is not responsible for the event that caused the damage.

Where multiple controllers or processors are involved, or both the controller and processor are responsible for the same processing, **all parties are jointly liable** for ensuring full compensation of the data subject's actual damage.

VII.5. Representation in Remedies and Judicial Proceedings

The data subject has the right to mandate a **non-profit body, organization, or association** whose statutes pursue public interest goals, particularly the protection of the rights and freedoms of data subjects with respect to their personal data, to represent them in proceedings.

Civil organizations can be found here: http://civil.info.hu/civil-szervezetek

---

VIII. Processing of Special Categories of Personal Data

Certain particularly sensitive personal data require special protection. The Company may process health-related data, such as:

- Social security identifiers of employees,
- Medical certificates related to occupational health fitness assessments,
- Medical documents required to verify entitlement to social security benefits.

These are handled **only to comply with legal obligations**, workplace health purposes, and assessment of work capacity or entitlement to benefits.

Special categories of personal data include:

- racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs,
- trade union membership,
- genetic and biometric data for unique identification,
- health data, and
- data concerning sex life or sexual orientation.

General rule: processing special categories of personal data is prohibited. The Company does **not** process special personal data.

Special personal data may be processed if:

- the data subject has given **explicit consent** for one or more specific purposes, except where EU or Member State law prohibits lifting the restriction via consent;
- processing is necessary to comply with legal obligations of the controller or data subject regarding employment, social security, or social protection, provided appropriate safeguards are in place;
- processing is necessary to protect **vital interests** of the data subject or another natural person where consent cannot be given;
- the data subject has **explicitly made the data public**.
- Processing is necessary for the **establishment, exercise, or defense of legal claims**, or when courts are acting in the exercise of their judicial authority.
- Processing is necessary for **preventive or occupational health purposes**, to assess the employee's ability to work, establish a medical diagnosis, provide health or social care or treatment, or manage health or social care systems and services, based on **EU or Member State law** or under a contract with a healthcare professional.

IX. Transfer of Data to Third Countries (Outside the EU):

The Company does **not currently transfer data abroad**, but sets out the following rules regarding such transfers.

The European Commission may decide, with effect across the Union, that a third country, a specific territory or sector of a third country, or an international organization provides an **adequate level of data protection**. In such cases, personal data may be transferred to the specified countries or international organizations **without requiring further authorization**(adequacy decision).

In the absence of an adequacy decision, the controller or processor is **required to provide appropriate safeguards** to compensate for the lack of data protection in the third country.

These safeguards ensure compliance with **data protection requirements** and provide data subjects with rights equivalent to those guaranteed within the EU, including enforceability of their rights and the availability of effective legal remedies.

SPECIFIC DATA PROCESSING ACTIVITIES OF THE COMPANY

1. REQUEST FOR OFFER

- **Purpose of processing:**
  - Contacting potential guests, maintaining further communication, identifying guests, distinguishing between guests, providing information about the services offered by the Data Controller, including prices and conditions.
- **Legal basis for processing:**
  - Voluntary consent of the data subject [GDPR Article 6(1)(a)].
- **Types of personal data processed:**
  - Name, email address, phone number.
- **Retention period:**
  - If the booking does not occur or is canceled without legal consequences, the data will be deleted immediately.
  - Until the guest withdraws their consent.
- **Possible consequences of not providing data:**
  - The Data Controller will not be able to provide an offer or information regarding the prices and conditions of the services.
- **Data transfer to processors:**
  - None.

---

2. BOOKING

- **Purpose of processing:**
  - Processing the room reservation request and reserving the specified room.
- **Legal basis for processing:**
  - Voluntary consent for contact details [GDPR Article 6(1)(a)].
- **Types of personal data processed:**
  - Name, email address, phone number.
- **Retention period:**
  - If the booking does not occur or is canceled without legal consequences, the data will be deleted immediately.
  - Until the guest withdraws their consent.
- **Method of processing:**
  - Online
  - By phone
  - In person
- **Possible consequences of not providing data:**
  - The reservation/contract for the specified room will not be created.
- **Data transfer to processors:**
  - None.

CHECK-IN / REGISTRATION

- **Purpose of processing:**
  - Reserving the specified room, issuing invoices, fulfilling accounting obligations, creating contracts, defining contract content, modifying contracts, monitoring contract performance, invoicing fees arising from contracts, enforcing related claims, fulfilling data reporting obligations, and maintaining records.
- **Legal basis for processing:**
  - Voluntary consent for contact details [GDPR Article 6(1)(a)]
  - Processing necessary for compliance with a legal obligation applicable to the Data Controller [GDPR Article 6(1)(c)] – Accounting Act §§ 159–169.
- **Types of personal data processed:**
  - Contact details: phone number and email address
  - For individual customers: personal identification data, including name, residential address, place and date of birth, ID card/passport number, as well as dates and times related to the booking/contract.
- **Retention period:**
  - Eight years, in accordance with Accounting Act § 169(2).
- **Possible consequences of not providing data:**
  - The individual will not be able to use the services provided by the Data Controller.
- **Data transfer to processors:**
  - None.

PROCESSING OF CONSUMER COMPLAINTS

- **Purpose of processing:**
  - Handling consumer complaints related to services provided by the Company in accordance with the Consumer Protection Act.
- **Legal basis for processing:**
  - Necessary for the performance of a contract [GDPR Article 6(1)(b)]
  - Necessary for compliance with a legal obligation applicable to the Data Controller [GDPR Article 6(1)(c)]
  - Consumer Protection Act § 17/A(7).
- **Types of personal data processed:**
  - Complaint unique identification number
  - Consumer name and address
  - Place, date, and method of complaint submission
  - Documents submitted or provided by the consumer and their list
  - Complaint description
  - Place, date, and name/signature of the person recording the minutes (if applicable)
  - Response letter following the investigation of the complaint
- **Retention period:**
  - Five years for copies of minutes and responses to written complaints, in accordance with Consumer Protection Act § 17/A(7).
- **Possible consequences of not providing data:**
  - The individual consumer cannot exercise their consumer rights.
- **Data transfer to processors:**
  - None.

ELECTRONIC SURVEILLANCE SYSTEM

- **Location and monitored areas:**
  The NN Boutique Hotel operates an electronic surveillance system (CCTV cameras) in the following locations:

Camera Location	Monitored Area
Main building, North corner	North vehicle entrance
Main building, NE corner	Access road to hotel
Main building, East corner	Eastern parking lot
Main building, East corner	Inner courtyard, terrace
Main building, South corner	Inner courtyard, terrace
Main building, South corner	Western parking lot
Main building, West side	Western parking lot
Kitchen, South corner	Western parking lot and entrance
Kitchen, West corner	Western parking lot
Kitchen, North corner	Kitchen entrance
Short wing corridor, ground floor middle	Corridor entrance front
Short wing corridor, ground floor middle	Corridor end
Café side wall	Reception, main entrance
Long wing corridor, ground floor middle	Corridor entrance front
Long wing corridor, ground floor middle	Corridor end
Restaurant, West wall	Restaurant counter and entrances
Restaurant, North wall	Restaurant counter and entrances
Short wing corridor, first floor middle	Corridor entrance front
Short wing corridor, first floor middle	Corridor end
Long wing corridor, first floor middle	Corridor entrance front
Long wing corridor, first floor middle	Corridor end
Conference room, East wall	Projector and screen

- **Purpose of processing:**
  - To protect human life, physical integrity, and property; to prevent, detect, and document violations; to identify unauthorized entrants; to record entries; to monitor activities of unauthorized persons; and to investigate workplace or other accidents on the NN Boutique Hotel premises.
- **Legal basis for processing:**
  - GDPR Article 6(1)(f): legitimate interest of the Data Controller in personal and property protection.
- **Types of personal data processed:**
  - Images of individuals entering the NN Boutique Hotel premises (facial images and other personal data captured by the surveillance system).
- **Retention period:**
  - 72 hours, unless a legitimate interest assessment by the Data Controller justifies a longer period, which must be documented and verifiable.
- **Access to recorded footage:**

    - Only authorized personnel may access recordings to prove violations affecting human life, physical integrity, or property, and to identify offenders.
- **Data transfers:**
    - To authorities in case of misdemeanors or criminal proceedings.

MARKETING PRESENCE ON SOCIAL MEDIA AND OWN WEBSITE

- **Social media presence:**
  The NN Boutique Hotel maintains a presence on:
    - Facebook: https://facebook.com/nnhotel.hu
    - Instagram: https://instagram.com/nn.boutique.hotel
    - TikTok: https://www.tiktok.com/@nn.boutique.hotel
- **Purpose of processing:**
    - To maintain social media presence and inform interested individuals about the NN Boutique Hotel and its services.
- **Data subjects:**
    - Any natural person who voluntarily follows, shares, or interacts with the Hotel's content on social media.
- **Legal basis for processing:**
    - Voluntary consent in accordance with GDPR Article 6(1)(a).
- **Types of personal data processed:**
    - Publicly visible name, profile information, photo, messages, reviews, or any other interactions performed by the data subject on the social media platform.
- **Retention period:**
    - Until the data subject withdraws their consent.
- **Possible consequences of not providing data:**
    - Not applicable, as the data is provided voluntarily by the data subject to the social media platform.
- **Data transfers to processors:**
    - None.
- **Additional information:**
    - Data subjects can read about the data processing policies of the respective social media platforms at:
        - Facebook: https://www.facebook.com/privacy/explanation/
        - Instagram: https://help.instagram.com/519522125107875/?helpref=hc_fnav