

DATA PROTECTION AND DATA MANAGEMENT SUPPORT

1. INTRODUCTION OF THE DATA CONTROLLER

HUNGUEST Hotels Hotel Industry Private Limited Company (hereinafter referred to as the "**Data Controller**") has created the following data protection notice to ensure the lawfulness of its internal data management processes and to safeguard the rights of data subjects.

Name of data controller: **HUNGUEST Hotels Hotel Industry Private Limited Company**

Company registration number of the Data Controller: **01-10-140409**

Registered office of the Data Controller: **1056 Budapest, Váci utca 38.**

E-mail address of the controller: **info@hunguesthotels.hu**

Representative of the Data Controller: **Ádám Détári-Szabó, CEO**

Data Protection Officer: **Kertész and Partners Law Office
(adatvedelem@hunguesthotels.hu)**

The Data Controller processes personal data in accordance with all applicable laws, but in particular with the following:

- Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information (hereinafter referred to as the "**Info Act**");
- Regulation (EU) 2016/679 of the European Parliament and of the Council 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 referred to as the "**Regulation**" or "**GDPR**").

The Data Controller shall treat personal data confidentially and shall take all technical and organisational measures related to data storage and management, and other technical and organisational measures to ensure the security of data.

2. DEFINITIONS

The terminology used in this Notice is identical to the interpretative definitions set out in Article 4 of the Regulation and to the interpretative provisions of Section 3 of the Info Act, supplemented at certain points.

When this Notice refers to data or processing, it means personal data or the processing thereof.

3. DESCRIPTION OF DATA PROCESSING

In order to operate in a lawful and prudent manner, the Data Controller shall, in accordance with the provisions of Act XXV of 2023 on Complaints, Whistleblowing and Rules Related to Whistleblowing (hereinafter referred to as the "**Complaints Act**"), set out its values and principles in the Code of Ethics and Business Conduct (hereinafter referred to as the "**Code of Ethics**"), the framework of conduct to be followed by its employees, other employees and partners, and the professional and ethical rules that ensure fair and responsible business conduct and good practice. In this way, the Data Controller aims to contribute to the establishment of a sound ethical basis for the operation of the company and to its long-term stability. The reputation and competitiveness of the Data Controller can only be maintained through integrity in business conduct and full compliance with the law, and non-compliance or even suspicion of non-compliance by employees and partners poses a significant reputational risk to the Data Controller, which may jeopardise business performance.

The Data Controller is also subject to the Complaints Act, given that it employs more than 50 people, and is therefore required to operate an internal whistleblowing system to receive and handle whistleblowing reports in accordance with the Complaints Act.

In view of the above, the Data Controller maintains an internal whistleblowing system for reporting - suspected - acts contrary to the law or to the standards of conduct or principles set out in the Code of Ethics or other internal regulations, in accordance with the provisions of the Complaints Act. This whistleblowing system may also be used to report breaches of rules of conduct (including ethical breaches) by the Data Controller that protect the public interest or substantial private interests, pursuant to Article 28 of the Complaints Act. The purpose of the operation of the notification system is thus to ensure compliance with the legal obligation and to ensure quality and efficient economic activity.

The rules of procedure for the submission of a whistleblowing report and the proceedings based on it, as well as the protection of whistle-blowers, are governed by the Code of Ethics and the Code of Procedures for Reporting Internal Misconduct (hereinafter referred to as the "**Code of Procedures**"), in accordance with the provisions of the Complaints Act.

The receipt of the report and the conduct of the proceedings based on the report also entail the processing of personal data by the Data Controller. The purpose of the processing, as set out above, is to ensure that a whistle-blower who has detected an activity (allegedly) in breach of the law or its regulations can make a notification, which will in any case be investigated by the Data Controller.

3.1. The purpose of data processing

The purpose of data processing is to operate the internal whistleblowing system, to detect and investigate illegal or suspected illegal acts or omissions, ethical breaches or other abuses and to conduct the relevant proceedings, in particular to ensure that reports are made, to investigate the reports and to remedy or terminate the conduct that is the subject of the report or to apply sanctions.

3.2. Persons concerned

Data subjects concerned by personal data processing are as follows:

- a) the person making a report or complaint to the Data Controller, i.e. the whistle-blower;
- b) the reported person against whom the report is made by the whistle-blower, and
- c) any other person concerned by the report, i.e. any person who otherwise participates in the procedure and who has substantive information on the subject matter of the reported incident.

3.3. Personal data processed

The Data Controller shall process the personal data of the whistle-blower and of the person concerned by the report that are indispensable for the investigation of the report, in particular,

1. the whistle-blower's name, postal address, telephone number and e-mail address;
2. data relating to the legal relationship (e.g. employment relationship, other legal relationship) on the basis of which the whistle-blower is acting in this capacity;
3. the content and date of the report,
4. a factual description of the conduct complained of, containing all relevant information necessary for the assessment of the case;
5. listing and attaching evidence, the record of the ethics hearing and other means of proof;
6. all data relating to the investigation of the report and the action taken on the basis of the investigation.

If the whistle-blower is a natural person, they must provide the data that allow the identification of the person, otherwise the Data Controller will treat the report anonymously and is not obliged to investigate it.

If the whistle-blower is a legal person, the report must be accompanied by the name of the legal person's registered office and the name of the legal representative submitting the report.

3.4. The legal basis for data processing

If the report qualifies as an ethical report, the legal basis for processing is legitimate interest within the meaning of Article 6(1)(f) of the Regulation. The Data Controller has a legitimate interest on the basis of the above

- a) to have the provisions of the Code of Ethics fully respected by the Data Controller's employees and contractors;
- b) to bring to light the conduct of persons who have breached the law and the ethical standards set out in the Code of Ethics;
- c) be able to determine and implement the necessary measures through the conduct of the procedure;
- d) that, if necessary, the Data Controller shall be able to conduct an investigation of the report;
- e) apply appropriate sanctions to persons who violate the law and the standards set out in the Code of Ethics.

If the report constitutes a report of abuse, the legal basis for processing is the fulfilment of the legal obligation of the Data Controller pursuant to Article 6 (1) (c) of the Regulation, arising from Section 18 (1) of the Complaints Act.

3.5. The source of personal data

The source of the data is the whistle-blower or the data subjects himself/herself in relation to the statements they made during the investigation.

3.6. The recipients of personal data made available

As set out in the Code of Procedures, personal data of a whistle-blower who discloses their identity may not be disclosed to persons other than those investigating the report.

The Data Controller may transfer the data to a lawyer or an external body assisting in the investigation of whistle-blowing for the purpose of investigating the whistle-blowing and remedying or stopping the conduct that is the subject of the notification. If the investigation of the conduct referred to in the report justifies the initiation of infringement or criminal proceedings, the Data Controller shall arrange for the filing of a complaint.

3.7. Data processor(s)

If the whistle-blower makes the report by e-mail and/or requests to receive information about the report by e-mail, the Data Controller will use the services of the following data processor:

The operator of the IT infrastructure (e-mail and IT Helpdesk)

MBIT TECHNOLOGICAL SERVICES LTD (registered office: 1117 Budapest, XI. Irinyi utca 4-20. B/3.)

The data processor may process the personal data of the data subject only for the purposes specified by the Data Controller and contractually agreed upon, in accordance with the Data Controller's instructions, and has no autonomous decision-making power with regard to the processing. The processor has undertaken confidentiality obligations and contractual guarantees with regard to the retention of personal data obtained in the course of its tasks.

3.8. The transfer of personal data to a third country or international organisation

The Data Controller shall not transfer personal data to third countries or international organisations.

3.9. The duration of processing of personal data

The Data Controller shall process the personal data within the limitation period after the final closure of the investigation.

3.10. Automated decision-making and profiling

Neither of these occurs during the processing.

3.11. The consequences of not providing data

If the report is received anonymously, without providing names, or if the identity of the whistle-blower cannot be identified on the basis of the data provided, the Data Controller is not obliged to carry out the investigation or may dispense with it.

4. THE RIGHTS OF THE DATA SUBJECT IN RELATION TO THE PROCESSING

4.1. The right to information

The data subject has the right to be informed about the processing of his or her personal data, which the Data Controller shall provide by means of this notice.

4.2. The right to access

At the request of the data subject, the Data Controller shall at any time inform the data subject whether or not their personal data are being processed and, if so, provide access to the personal data and the following information:

- a) the purposes of the processing;

- b) the categories of personal data concerned;
- c) the recipients or categories of recipients to whom or with which the Controller has disclosed or will disclose the personal data, including in particular recipients in third countries or international organisations;
- d) the envisaged period of storage of the personal data or, if this is not possible, the criteria for determining that period;
- e) the data subject shall also be informed of his or her right to obtain from the Controller the rectification, erasure or restriction of the processing of personal data concerning him or her and to object to the processing of such personal data;
- f) the right to lodge a complaint with a supervisory authority or to take legal action;
- g) where the data have not been collected directly from the data subject by the Data Controller, any available information on the source of the data;
- h) where automated decision-making is carried out, the fact of such processing, including profiling, and, at least in those cases, the logic used, i.e. the significance of such processing and the likely consequences for the data subject.

4.3. The right to rectification of personal data

The data subject shall have the right at any time, upon request and without undue delay, to obtain from the Data Controller the rectification of inaccurate personal data relating to him or her. Taking into account the purpose of the processing, the data subject shall also have the right to request the completion of incomplete personal data, including by means of a supplementary declaration.

In the case of a request for rectification (amendment) of data, the data subject must substantiate the accuracy of the data requested to be amended and must also certify that the person entitled to the amendment is the person who requests the amendment. Only in this way can the Data Controller assess whether the new data is accurate and, if so, whether it can amend the previous data.

The Data Controller further draws the attention of the data subject to the need to notify any change in his/her personal data as soon as possible, thus facilitating lawful processing and the exercise of his/her rights.

4.4. The right to erasure

At the request of the data subject, the Data Controller shall delete personal data concerning the data subject without undue delay where one of the following grounds applies:

- a) the Controller no longer needs the personal data for the purposes for which they were collected or otherwise processed;

- b) where processing is based on consent, the data subject withdraws the consent on which the processing is based and there is no other legal basis for the processing;
- c) the data subject objects to the processing and there are no overriding legitimate grounds for the processing or objects to processing for direct marketing purposes;
- d) the personal data are unlawfully processed by the Controller;
- e) the personal data must be erased in order to comply with a legal obligation under Union or Member State law applicable to the Data Controller;
- f) personal data are collected in connection with the provision of information society services.

4.5. The right to restriction of processing

The data subject shall have the right to obtain, at his or her request, the restriction of processing by the Controller if one of the following conditions is met:

- a) they contest the accuracy of the personal data; in this case, the restriction applies for the period of time that allows the Controller to verify the accuracy of the personal data;
- b) the data processing is unlawful and they oppose the erasure of the data and instead request the restriction of their use;
- c) the controller no longer needs the personal data for the purposes of processing, but the data subject requires them for the establishment, exercise or defence of legal claims; or
- d) the data subject has objected to the processing; in this case, the restriction applies for the period until it is established whether the legitimate grounds of the Controller prevail over the legitimate grounds of the data subject.

4.6. The right to object

Where the processing of personal data is based on the legitimate interests of the controller [Article 6(1)(f) of the Regulation] or is necessary for the performance of a task carried out in the exercise of official authority vested in the controller [Article 6(1)(e) of the Regulation], the data subject shall have the right to object at any time, on grounds relating to his or her particular situation, to processing of his or her personal data, including profiling based on those provisions.

4.7. Interest screening test

Where the legal basis for the processing of personal data is the legitimate interest of the controller or a third party within the meaning of Article 6(1)(f) of the Regulation, a written "balancing of interests test" will be carried out in accordance with preamble Article 47 and Article 5(2), which the data subject may request by sending an e-mail to adatvedelem@hunguesthotels.hu.

5. THE PROCEDURES FOR ENFORCING THE RIGHTS OF THE DATA SUBJECT

The data subject may exercise the above rights by sending an e-mail to adatvedelem@hunguesthotels.hu, by post to the Data Controller's head office or by visiting the Data Controller's head office in person. The Controller shall investigate and act on the data subject's request without undue delay after receipt of the request. The Controller shall inform the data subject of the action taken on the basis of the request within 30 days of receipt. If the Controller is unable to comply with the request, it shall inform the data subject of the reasons for the refusal and of his or her rights of appeal within 30 days.

Within five years after the death of the data subject, the rights of the deceased as set out in this notice, which the data subject enjoyed during his or her lifetime, may be exercised by a person authorised by the data subject by means of an administrative arrangement or a declaration in a public or private document of full probative value made to the controller or, if the data subject made several declarations to a controller, by a declaration made at a later date. Even if the data subject has not made a corresponding declaration, his or her close relative within the meaning of the Civil Code shall still be entitled to exercise the rights under Articles 16 (right to rectification) and 21 (right to object) of the Regulation and, where the processing was unlawful during the data subject's lifetime or the purpose of the processing ceased to exist upon the death of the data subject, under Article 17 (right to access) of the Regulation (right to erasure) and 18 (right to restriction of processing) of the Regulation within five years of the death of the data subject. The right to exercise the rights of the data subject under this paragraph shall be exercised by the next of kin who first exercises that right.

6. THE RIGHT TO A JUDICIAL REMEDY IN RELATION TO DATA MANAGEMENT

In order to enforce his or her right to judicial remedy, the data subject may take legal action against the Controller if he or she considers that the processing of his or her personal data by the Controller or by a processor or joint controller acting on our behalf or on our instructions is in breach of the requirements laid down by law or by a binding legal act of the European Union for the processing of personal data. The court will decide the case out of turn. The Tribunal has jurisdiction to hear the case. The action may be brought, at the option of the data subject, before the court of the place of residence or domicile of the data subject or before the court of the place where the Controller has its registered office (Budapest-Capital Regional Court).

Anyone may file a complaint with the National Authority for Data Protection and Freedom of Information (in Hungarian: NAIH) against the Data Controller, alleging that the processing of personal data has resulted in a violation of rights or an imminent threat thereof, or that the Data Controller is restricting the exercise of rights related to the processing of personal data or is refusing to exercise such rights. The notification can be made using one of the following contact details:

National Authority for Data Protection and Freedom of Information (NAIH)
Postal address: 1363 Budapest, Pf. 9.
Address: 1055 Budapest, Falk Miksa utca 9-11.
E-mail: ugyfelszolgalat@naih.hu
URL: <http://naih.hu>

Budapest, 24 July, 2023.