BUDA CASTLE
FASHION HOTEL

CAMERA POLICY

On the management of personal data by means of a video recording device

1. PURPOSE AND SCOPE OF THE POLICY

The purpose of present camera policy (hereinafter referred to as: „**Policy**") is to determine and provide information about the lawful order of the use of the video capture equipment (CCTV's) operated by the **Mellow Mood Hungary Kft.** (hereinafter referred to as: „**Controller**") in the building of the Buda Castle Fashion Hotel (hereinafter referred to as: „**Hotel**"). The purpose of this Policy is also to ensure that the constitutional principles of data protection, the right to self-determination and data security are upheld, and to allow for the data subjects to have control over their data, to learn about the circumstances under which the data are processed and to prevent unauthorized access, alteration or disclosure. Present Policy is subject to the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, hereinafter referred to as "**GDPR**").

2. DATA OF THE CONTROLLER

Applicable data of the Collector are the followings:

- Name: **Mellow Mood Hungary Kft.**
- Seat: **1077 Budapest, Baross Gábor tér 15. 5. em. 1.**
- Company Reg. No.: **01-09-873388**
- VAT-No.: **13791018-2-42**
- Registering court: **Budapest-Capital Regional Court**
- Telephone number: **+36 1 224 7900**
- E-mail: **reception@budacastlehotelbudapest.com**
- Data Protection Officer: **dr. Pozsgay Péter**
- E-mail address of DPO: **office@drpozsgaypeter.hu**
- Telephone number of DPO: **+36 20 5574 860**

3. SCOPE, PURPOSE, DURATION, TITLE, DELETION DEADLINE AND FORWARDING OF PROCESSED DATA

Processed data: **Video recording (image only) of the behavior of those staying in the Hotel's customer traffic areas, which are open to the public. Sound will not be recorded by the Controller.**

Purpose of data processing: **To protect the property, physical integrity and other legitimate interests of its guests, its employees, its own and any third parties, and to facilitate the enforcement of the data subjects' rights.**

Legal title of data processing: **the legitimate interest of the Controller, the data subjects and the society regarding the security of property and life (Article 6 (1) (f) of GDPR). The Controller proved the existence of its legitimate interest in a separate legitimate interests assessment.**

Deadline of deletion of data: **They are automatically deleted 72 hours after recording. Further processing of data may only occur if it is required for enforcing the rights of the data subject, the Controller or other third parties, or where there is a suspicion that such recording may be necessary to enforce the rights of any person.**

4. PRINCIPLES GOVERNING THE PROCESSING OF PERSONAL DATA

(a) Processing of personal data is carried out by the Controller in a lawful and fair manner, in a manner that is transparent to the data subject ("**Lawfulness, Fairness and Transparency**"). The most important information shall be disclosed on warning signs. These signs shall be located at a sufficient distance from the observed area so that the person(s) concerned can easily obtain information on the circumstances of the observation before entering the area.

(b) The Controller only collects personal data for the purposes set out in present Policy, for a clear and legitimate purpose, and processes them in a manner consistent with that purpose. ("**Purpose Limitation**")

(c) The personal data must be adequate and relevant to the purposes for which the data are processed and must be limited to what is necessary. Prior to installing the CCTV, Controller shall verify that it is suitable, appropriate and necessary to achieve its purpose. A camera surveillance system may be installed where the purpose of data management cannot be attained in a way which does not interfere with the data subject's fundamental rights and freedoms. ("**Data Minimisation**")

(d) All personal data shall be kept in a form which permits identification of data subject(s) only for as long as is necessary for the purposes for which the personal data are processed. ("**Storage Limitation**")

(e) The Controller shall ensure that personal data are adequately protected by appropriate technical or organizational measures, including protection against unauthorized or unlawful processing, accidental loss, destruction or damage. ("**Integrity and confidentiality**")

(f) The Controller shall be responsible for compliance with (a) to (e) and shall be able to justify such compliance. ("**Accountability**")

The cameras monitor the entire area of the Hotel which is open for client traffic, as well as the facade and street front of the Hotel, including the street parking spaces reserved for it. Specifying the exact location and angle of view of the cameras is not compatible with the purpose of data management and is therefore not published in the Policy.

5. RIGHTS OF DATA SUBJECT, REMEDIES

5.1 Right to information and access

On the request of the data subject, the Controller shall provide the data subject to the following information:

(a) Whether the personal data of the data subject are being processed by the Controller;

(b) the name and contact details of the Controller;

(c) the personal data managed by the Controller concerned and the source thereof;

(d) the purpose of the processing of personal data and the legal basis for the processing;

(e) the duration of the processing;

(f) the recipients or categories of recipients to whom the personal data have been or will be communicated, including in particular third-country recipients or international organizations;

(g) the consequences of data processing;

(h) the rights of the data subject;

(i) the circumstances, the effects and the measures taken to deal with any data protection incident.

If a record of the data subject is stored, the data subject(s) have the right of access under Article 15 of the GDPR. The right to request a copy shall not adversely affect the rights and freedoms of others. In some cases, the Controller may not issue footage that identifies others. However, in order to ensure that the rights and freedoms of others are not impaired, the right of access shall be guaranteed by the Controller employing a technical solution, a means by which he/she fulfills his/her right of access. If the video cannot be searched for personal data, the Controller will not be able to identify the data subject. Therefore, the subject must accurately identify (by a timeframe) when he/she was entering the monitored area. If the Controller cannot identify the data subject, the data subject shall be informed about that.

5.2 Right to object

The data subject(s) shall have the right at any time to object to the processing of data for reasons related to their own situation(s). In the case of camera surveillance, objects may take place before, during or after entering the surveillance area. If the data subject exercises his/her right to object, the Controller shall act in accordance with Article 21 of the GDPR.

5.3 Right of rectification:

The data subject may request correction of inaccurate data managed by the Controller.

5.4 Right of cancellation:

If any of the following reasons exist, the Controller shall, upon request of the data subject, delete the data relating to the data subject as soon as possible, but at the latest within 5 working days:

(a) The data has been processed unlawfully (without legal authorization or personal consent);

(b) data management is not necessary for the original purpose;

(c) the data subject withdraws his consent to data processing and the Data Controller has no other legal basis for data processing;

(d) the data in question were collected in connection with the provision of information society services;

(e) personal data must be deleted in order to comply with the data controller's legal obligations.

The Controller will not be able to delete the data if the data processing is still required for any of the following:

(a) Necessary for the exercise of the right of expression and information;

(b) the public interest;

(c) for archival, scientific, research or statistical purposes;

(d) to assert or defend legal claims.

5.5 Right to Restrict Data Management:

If any of the following reasons exist, the Controller shall restrict the processing of the data to the request of data subject:

(a) The data subject disputes the accuracy of the data concerning him, in which case the limitation applies to the time until the accuracy and correctness of the data in question is credibly reviewed;

(b) the data processing is unlawful, but the data subject insists on the deletion, but only on the restriction of data processing;

(c) the data are no longer needed for data management, but the data subject requests that they be further stored to enforce or protect their legal claims.

If the Controller imposes a restriction on any of the data handled, then during the duration of the restriction, the Data Controller shall only handle the data concerned to the extent that:

(a) The data subject shall contribute to this;

(b) necessary for the enforcement or defense of legal claims;

(c) necessary to assert or defend the rights of another person;

(d) necessary for the protection of the public interest.

5.6 Right to data portability:

The data subject shall have the right to request the Controller to transfer the data concerning him or her to another data controller in a commonly used computer software readable format. The request will be complied with by the Controller as soon as possible and at the latest within 30 days.

5.7 Remedies:

(a) If you have any concerns about the privacy issues of the Controller, please do not hesitate to contact the **Data Protection Officer of the Controller, dr. To Péter Pozsgay** (contact: office@drpozsgaypeter.hu; +36 20 5574 860).

(b) If, in the opinion of the data subject, his/her rights have been violated by the Controller and/or the data processor(s), he/she shall be entitled to apply to the court with jurisdiction and competence in accordance with the Code of Civil Procedure. The court acts in such cases promptly.

(c) If the data subject wishes to file a complaint in respect of the data processing, he/she may turn to the Hungarian National Authority for Data Protection and Freedom of Information as follows: seat: 1125 Budapest, Szilágyi Erzsébet fasor 22/C.; postal address: 1530 Budapest, Pf.: 5. telephone number: +36 1 391 1400; fax: +36 1 391 1410; e-mail address: ugyfelszolgalat@naih.hu; website: www.naih.hu.

Date: Budapest, 2 December 2019