The Three Corners Europe Hotel Management Kft.

Three Corners Hotel Anna***

CAMERA PRIVACY POLICY

Introduction

Pursuant to Articles 12 and 13 of 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 the GDPR), **The Three Corners Europe Hotel Management Kft.** (hereinafter: Data Controller) **provides the** following information to the data subjects regarding the data processing carried out by the Data Controller with cameras installed in the Hotel.

The purpose of this Privacy Policy is to provide information to the data subjects in an easily understandable form about the principles followed by the Data Controller when processing their personal data, the rights to which they are entitled and the main data processing rules. These rules are contained in this Privacy Policy of the Data Controller, defining the main characteristics of the Data Controller's data processing.

I. DATA AND CONTACT DETAILS OF THE DATA CONTROLLER, PERSONAL DATA AND THE CONCEPT OF THE DATA SUBJECT

Name of the data controller	**The Three Corners Europe Hotel Management Kft.**
Registered office of the Data Controller:	1163 Budapest, Margit u. 45.
Address of the Hotel:	Gyulai Pál utca 14., 1085, Budapest, Hungary
Contact details of the Data Protection Officer	adatjogvedo@outlook.hu,
Phone number (customer service)	+ 36/30 327 49 33
Availability of data protection documents	Physical: posted at the reception

For the purposes of this policy, personal data is any information relating to a natural person (the Data Subject) by which the Data Subject can be identified.

II. DESCRIPTION OF THE DATA PROCESSING PROCESS, DETAILED PRESENTATION OF THE PURPOSES OF DATA PROCESSING, THE LAWS SERVING AS THE BASIS FOR DATA PROCESSING

This Policy applies to the data processing of surveillance carried out with cameras in the area of the Hotel operated by the Data Controller (address: 1053 Budapest, Királyi Pál utca 12.).
The purpose of the operation of the camera surveillance system is to prevent and prove the commission of unlawful acts, thus realizing the

a) protection of the life and physical integrity of persons entering or staying in the area owned or used by the Data Controller and monitored by cameras (hereinafter referred to as: monitored area), and
b) protection of buildings, movable property, equipment, vehicles located in the monitored area, as well as the property of persons entering and staying in the monitored area (from burglary, theft or vandalism),
c) Protection of the personal safety and physical integrity of the hotel's customers/guests and the employees of the Hotel.

Surveillance and recording carried out with cameras equipped in the area of the Hotel operated by the Data Controller is carried out on the basis of the legitimate interest of the Data Controller pursuant to Article 6 (1) (f) of the GDPR. During the application of the camera surveillance system, personal data may be processed to the extent strictly necessary for the realization of the purpose of data processing. The cameras only record moving images. Sound recordings – together with video recordings – are not recorded with regard to data processing based on legitimate interest.

The cameras are not used for direct observation in addition to recording the recordings. The Data Controller performs recorded surveillance, which means that the recordings are only viewed if an event has occurred in accordance with the purpose of the recording, or if the data subject has submitted an access request to the Data Controller, in which he or she requested the viewing of the recording or the release of a copy of the recording. In the future, the Data Controller will only use the recordings for the purpose of investigating an event internally, or in judicial or official proceedings. In the event of the initiation of an official or judicial proceeding or a request, the Data Controller shall make a copy of the recordings, which shall be forwarded exclusively to the body proceeding in the case.

The primary task of the Data Controller is to determine the scope of the personal data processed, the legal basis and purpose of data processing, the means and method of data processing, as well as to ensure the enforcement of the constitutional principles of data protection and the requirements of data security, and to prevent unauthorized access to personal data, the alteration and unauthorized disclosure or use of data, as well as to ensure protection against deletion, damage and destruction.

The main legal regulations on data processing under this Policy and their abbreviations used in this Policy:

- 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); GDPR)

III. SOURCE AND PROCESSING OF INDIVIDUAL PERSONAL DATA, LEGAL BASIS OF DATA PROCESSING, SCOPE OF DATA PROCESSED, DURATION OF DATA PROCESSING

Name and purpose of data processing	Legal basis for data processing	Personal data processed Circle	Duration of data processing
1. Surveillance and recording with a camera in the Hotel operated by the Data Controller for the purpose of personal and property protection, for the purpose of protecting the personal safety and physical integrity of the hotel's customers/guests and our Hotel employees, as well as for the protection of buildings, movable property, equipment, vehicles, as well as the property of persons entering and staying in the monitored area (from burglary, theft or vandalism).	Legitimate interest of the controller within the meaning of Article 6(1)(f) of the GDPR.	Image of data subjects (Image and video recording of data subjects)	The Data Controller stores the recordings for 8 days, after which the recordings are deleted.
2. Storage of recordings for the purpose of internal investigation of the event recorded by cameras installed in the Hotel area.	Legitimate interest of the controller within the meaning of Article 6(1)(f) of the GDPR.	Image of data subjects (Image and video recording of data subjects)	The recordings will be deleted on the 15th day after the completion of the internal investigation.
3. Storage, copying and forwarding of the recordings for the purpose of investigating the event recorded by cameras installed in the Hotel area in court or official proceedings.	Legitimate interest of the controller within the meaning of Article 6(1)(f) of the GDPR.	Image of data subjects (Image and video recording of data subjects)	Recordings until 15 days after receipt of the notification of the entry into force or finality of the decision closing the judicial or administrative proceedings

Results of the balancing of interests test carried out by the Data Controllers:

Legitimate interest exists	The legitimate interest is duly defined, genuine and current, as the data processing is actually necessary for the communication of the Data Controller's activities to the public.
Data processing is necessary	Data processing is necessary for the realization of legitimate interest, since in the absence of such a process, the Data Controller's goal - to ensure the protection of the personal safety and physical integrity of the Hotel's customers/guests and our Hotel employees, as well as the protection of buildings, movable property, equipment, vehicles and the property of persons entering and staying in the monitored area (from burglary, theft or vandalism) - could not be achieved.
Data processing constitutes a proportionate restriction with regard to the data subject	In the course of Data Processing, the interests, fundamental rights and freedoms of the Data Subjects are not violated. Compared to the interests of the Data Controller, the interests of the Data Subject do not enjoy a higher level of protection. With regard to the fact that the Data Subject receives the appropriate information about the data processing concerning him or her at the time of data collection, and that the effects of data processing are fully predictable due to the method of data processing, the measure of proportionality in this respect is shifting towards the permissibility of data processing. The proportionality of the restriction is also increased by the fact that the data controller provides the data subject with comprehensive, clear and comprehensible information at the time of data collection about the scope of the personal data processed, the basis, method and time of data processing, and the data subject's rights related to data processing.

With regard to the provisions of Article 21 of the GDPR, the Data Controller clearly and separately from any other information expressly draws the attention of the Data Subject to the fact that each Data Subject has the right to object at any time to the processing of his or her personal data based on Article 6(1)(f) of the GDPR for the purposes of data processing specified in this Policy, on grounds relating to his or her particular situation.

In this case, the Data Controller may no longer process the personal data, unless the Data Controller proves that the data processing is justified by compelling legitimate grounds that take precedence over the interests, rights and freedoms of the Data Subject, or that are related to the establishment, exercise or defence of legal claims.

IV. THE FACT OF AUTOMATED DECISION-MAKING, including profiling, as well as, at least in these cases, comprehensible information about the logic used and the significance of such processing and the expected consequences for the data subject:

No automated decision-making or profiling takes place during the processing of personal data detailed in this Privacy Policy.

V. DATA SECURITY MEASURES

The Data Controller undertakes to ensure the security of the personal data it processes. Taking into account the state of science and technology and the costs of implementation, as well as the nature, scope, circumstances and purposes of the processing, as well as the risks to the rights and freedoms of natural persons of varying probability and severity, it shall take the technical and organisational measures and establish the procedural rules to ensure that the data recorded, stored or processed are protected, or prevent their destruction, unauthorized use and unauthorized alteration.

The Data Controller also undertakes to call upon all third parties to whom the data are forwarded or transferred on any legal basis to comply with the requirement of data security.

The Data Controller shall guarantee a level of data security appropriate to the degree of risk, including, inter alia, where applicable:

- pseudonymization and encryption of personal data,
- ensuring the continued confidentiality, integrity, availability and resilience of the systems and services used to process personal data (operational and development security, intrusion protection and detection, prevention of unauthorised access),
- in the event of a physical or technical incident, the ability to restore access to and availability of personal data in a timely manner (prevention of data leakage; vulnerability and incident management);
- a procedure for regularly testing, assessing and evaluating the effectiveness of the technical and organizational measures taken to guarantee the security of data processing (maintaining business continuity, protecting against malicious codes, securely storing, transmitting and processing data, security training of our employees).

When determining the appropriate level of security, the risks arising from the processing of personal data shall be expressly taken into account, in particular from the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

The Data Subject's data is stored on the protected internal servers of the Data Controller, which is protected by the highest IT security standards. Remote access is only possible for a limited number of authorized persons, only through a virtual private network, after authentication. All operations performed by the User and the Service Provider related to data processing involving modifications will be logged. The data will not be copied to any other physical medium.

The Data Controller operates the IT tools used for the processing of the recorded personal data as follows:

- To ensure the protection of physical devices that contain data relating to the Data Controller.
- To ensure that only approved and authorized Users have access to the data used by the Data Controller.
- To ensure that only persons authorised to use the systems have access to the Data Controller's data.
- To ensure that the Data Controller's data cannot be transmitted, read, modified or deleted by an unauthorised person during data transmission or storage. The managed data shall only be accessed

by the Managing Director acting on behalf of the Data Controller and the Hotel Director, in such a way that they may not disclose them to persons who are not entitled to access the data.

- To ensure that the Data Controller's data is protected from accidental destruction or loss, and in the event of events that trigger these consequences, they have timely access to and restore the Data Controller's data.
- To ensure that the Data Controller's data is processed separately from the data of other customers. The Data Controller classifies and manages personal data as confidential data. In order to protect the data files electronically managed in the various registers, the Data Controller shall ensure that the data stored in the registers – with the exceptions specified by law – cannot be directly linked and assigned to the Data Subject.
- In order to ensure the security of IT systems, the Data Controller protects the IT systems with a firewall, and uses antivirus and anti-virus software to prevent external and internal data losses. The Data Controller has also ensured that incoming and outgoing communication in any form is properly controlled in order to prevent abuse.

VI. DATA PROCESSORS, DATA TRANSFER

Name and registered office of the data processor	**Activity performed by a data processor**	**Personal data processed by the data processor**
	operation and maintenance of the hotel's camera system	Camera footage

VII. YOUR (DATA SUBJECT'S) RIGHTS AND THE ORDER OF THEIR ENFORCEMENT:

The Data Controller shall inform the Data Subject without undue delay, but within one month of the receipt of the request, of the measures taken in response to the following request at the contact details provided by the Data Controller. If necessary, taking into account the complexity of the application and the number of applications, this deadline may be extended by a further two months. The data controller shall inform the data subject of the extension of the deadline within one month of receipt of the request, indicating the reasons for the delay.

<u>You, as a data subject, can exercise your rights below at the following contact details:</u>

<u>In person:</u>
At the registered office of the Data Controller (1163 Budapest, Margit u. 45.)

<u>in writing:</u>
\u2012 electronically (e-mail): adatjogvedo@outlook.hu,
\u2012 by phone: 30/327 49 33

<u>Your right to information</u>

The Data Controller is obliged to provide the Data Subjects with the following information on data processing at the time of obtaining the personal data, if the personal data originate from the Data Subject:

a) the name, contact details and representative of the Data Controller;
b) contact details of the Data Protection Officer;
c) the purpose of the planned processing of personal data and the legal basis for the processing;
d) in the case of data processing based on legitimate interests, the legitimate interests of the Data Controller or a third party; e) the recipients of the personal data;
f) the duration of the storage of the personal data;
g) whether the controller intends to transfer the personal data to a third country or to an international organisation;
h) informing about the rights of the Data Subject;
i) the right to withdraw consent in the case of data processing based on consent;
j) the right to lodge a complaint with a supervisory authority;
k) whether the provision of personal data is based on a law, a contractual obligation or a prerequisite for entering into a contract;
l) the fact of automated decision-making, including profiling,

The obligation to provide information described above does not have to be fulfilled if the Data Subject already has the information included in these sections.

If the personal data were not obtained from the Data Subject, the Data Controller shall provide the Data Subject with the above information, as well as the following information in addition to them:

a) the categories of Personal Data Covered;
b) the source of the personal data and, where applicable, whether the data originated from publicly available sources.

If the personal data were not obtained from the Data Subject, the obligation to provide information does not have to be fulfilled if:

- the Data Subject already has the information,
- the provision of information proves impossible or would require a disproportionate effort;
- the acquisition or disclosure of the data is expressly required by the EU law or the Hungarian law applicable to the Data Controller, or
- Personal data must remain confidential on the basis of a professional secrecy obligation imposed by EU or applicable Hungarian law.

Your right of access

You have the right to receive feedback from the Data Controller as to whether your personal data is being processed and, if such processing is in progress, you have the right to access the personal data and the following information: a) the purposes of the processing;
b) the categories of personal data we process about you;
c) the recipients or categories of recipients to whom the Personal Data are or will be communicated by the Data Controller, including, in particular, recipients from third countries or international organisations;

d) where applicable, the envisaged period for which the personal data will be stored or, if this is not possible, the criteria for determining that period;
e) your right to request the Controller to rectify, erase or restrict the processing of personal data concerning you and to object to the processing of such personal data;
f) to a supervisory authority (in Hungary) a National Data Protection and the Freedom of Information Authority);
g) if the data was not collected from you by the Data Controller, all available information on their source;
h) the fact of automated decision-making, including profiling, and, at least in these cases, comprehensible information about the logic used and the significance of such processing and the likely consequences for you.

The Data Controller will provide you with a copy of the personal data that is the subject of data processing. The Data Controller may charge a reasonable fee based on administrative costs for any additional copies requested by you. If you have submitted your application electronically, the information must be provided in a commonly used electronic format, unless you request otherwise. The right to request a copy must not adversely affect the rights and freedoms of others.

You may request access to or request copies of your recordings within the retention period of the camera recording. In your application, you must indicate on which day and when (at what hour and minute) the recordings were made, which cameras you wish to view or from which recordings you wish to have access, and on which day you wish to access the recordings.

In his application, the data subject may indicate a time during working hours for the inspection. Inspection is possible at the registered office of the Data Controller. The Data Controller draws your attention to the fact that if you do not exercise the opportunity of access within 8 days of receiving your request, the Data Controller will delete the recording.

Your right to rectification or completion

Upon your request, the Data Controller is obliged to rectify any inaccurate personal data concerning you without undue delay. Taking into account the purpose of data processing, you have the right to request the completion of incomplete personal data, including by means of a supplementary statement.

Your right to erasure

You have the right to request the Data Controller to delete the personal data concerning you. The Data Controller is obliged to delete the personal data concerning you without undue delay in the following cases:
a) the personal data is no longer necessary for the purposes for which it was collected or otherwise processed;
b) You object to the processing of your data in the legitimate interests of the data controller (third party) and there is no overriding legitimate reason for the processing;

The deletion request cannot be fulfilled if the data processing:
a) it is necessary for the submission, exercise or defence of legal claims.

Your right to block (restrict processing)

You have the right to request the Data Controller to restrict data processing if one of the following applies:

a) you contest the accuracy of the personal data, in which case the restriction applies to the period that allows the Data Controller to verify the accuracy of the personal data;
b) the processing is unlawful and you oppose the erasure of the data and instead request the restriction of its use;
c) the Data Controller no longer needs the personal data for the purposes of data processing, but you require them for the establishment, exercise or defence of legal claims, or
d) the data subject objected to the data processing, in which case the restriction lasts until the Data Controller determines whether its legitimate interests take precedence over the data subject's rights.

Where processing is restricted on the basis of the above, such personal data, with the exception of storage, may only be processed with your consent, or for the establishment, exercise or defence of legal claims, or for the protection of the rights of another natural or legal person, or for reasons of important public interest of the Union or of a Member State.

The Data Controller informs you in advance – at whose request the data processing has been restricted – about the lifting of the restriction of data processing. The blocking lasts as long as the reason you have indicated requires the storage of the data.

For example, you may request the blocking of your data if you believe that your data have been unlawfully processed by the Data Controller, but it is necessary for the sake of the official or judicial proceedings initiated by the Data Controller that the Data Controller does not delete them. In this case, the Data Controller will continue to store the personal data until the authority or the court is contacted, after which the data will be deleted.

You can request that recordings be blocked within the retention period. In your application, you must indicate – on which day and when (at what time) and within what time interval the recording was made, and – which cameras you request to be locked – for what reason you request the blocking of the recording.

The submission of the request is supported by a form, which is available at the security service or can be downloaded from the website of the Data Controller. The Data Controller will respond to your request within 1 month. In justified cases, the Data Controller will block the recording indicated by you for an additional 1 month.

Your right to object

You may object to the processing of your personal data if the legal basis for the processing is:

- the legitimate interest of the Data Controller or a third party pursuant to Article 6(1)(f) of the GDPR.

In the case of exercising the right of objection, the Data Controller may no longer process the personal data, unless it proves that the data processing is justified by compelling legitimate reasons that take precedence over the interests and rights of the Data Subject or that are related to the submission, exercise or defence of legal claims.

Your right to legal remedy

Contacting the Data Controller

We recommend that before initiating a court or official procedure, please send your inquiry or complaint related to the processing of your personal data to the Data Controller, so that we can investigate and remedy it satisfactorily, and we can fulfil any of your requests or requests under the previous point, if it is justified.

In the event of the enforcement of the Data Subject's right in relation to data processing as specified in the previous point, the request for information related to data processing, or the objection and complaint related to data processing, the Data Controller shall investigate the case without undue delay, within the time prescribed by the prevailing legislation, take measures in connection with the inquiry and provide information on the matter to the Data Subject. If necessary, taking into account the complexity of the request and the number of requests, this deadline may be extended as provided for by law.

If the Data Subject submitted the request electronically, the Data Controller shall provide the information electronically if possible, unless the Data Subject requests otherwise. If the Data Controller does not take action on the basis of the Data Subject's request without delay, but no later than within the deadline specified by law, it shall inform the Data Subject of the reasons for the failure to take action, the refusal to comply with the request, and of the fact that the Data Subject may initiate court or official proceedings in his or her case as follows.

In order to enforce your rights related to data processing, or if you have any questions or doubts about your data processed by the Data Controller, or if you request information about your data, wish to file a complaint or wish to exercise any of your rights under the previous point, the Data Controller may do so by 1.) .

Initiating court proceedings

The Data Subject may turn to court against the Data Controller if he/she considers that the Data Controller processes his/her personal data in violation of the provisions on the processing of personal data specified in legislation or in a binding legal act of the European Union.
The adjudication of the lawsuit falls within the jurisdiction of the General Court. The lawsuit may also be initiated before the competent court of the Data Subject's place of residence or residence, at the choice of the Data Subject. You may also initiate a civil lawsuit against the Data Controller. The Court of Justice shall have jurisdiction to hear the lawsuit. In principle, the lawsuit can be initiated before the Metropolitan Court of Budapest with jurisdiction over the registered office of the Data Controller, and also – at your choice – before the regional court of your place of residence.

Lodge a complaint with the supervisory authority
If you believe that your data are being processed unlawfully by the Data Controller – without prejudice to other administrative or judicial remedies –, you have the right to lodge a complaint with the National Authority for Data Protection and Freedom of Information (NAIH) (address: 1055 Budapest, Falk Miksa utca 9-11., postal address: 1363 Budapest, Pf. 9., e-mail: ugyfelszolgalatnaih.hu, phone: +36 (1) 391-1400, fax: +36 (1) 391-1410, website: www.naih.hu) – in particular in the Member State of your habitual residence, place of work or place of the alleged infringement – if in the opinion of the Data Controller restricts the enforcement of its rights or rejects its request for the enforcement of these

rights (initiation of an investigation), and if in the course of the processing of your personal data, the Data Controller or the data processor commissioned or acting on the basis of the Data Controller infringes the data protection rules on the processing of personal data, the requirements laid down in a law or a binding legal act of the European Union (request for an administrative procedure).

Privacy Policy **10/02/2026** effective from the date of the meeting.

The Three Corners Europe Hotel
Management Kft.
Mr. Didier Cormelius Lambrecht
Managing Director