INTERNAL DIRECTIVES

The hotel operator

FAIRHOTEL s.r.o., Rybářská 202, 60300 Brno, 01611623, CZ01611623

on the protection of personal data

The hotel operator FAIRHOTEL s.r.o. with registered office at Rybářská 202, 60300 Brno, 01611623, CZ01611623 (hereinafter referred to as the "**Operator**"), issues the following internal directive for the protection of personal data (hereinafter referred to as the "**Directive**").

1. PURPOSE OF THE DIRECTIVE

1.1. The purpose of this Directive is to regulate the protection of personal data and to establish binding rules for the processing of personal data by the Operator as a personal data controller, especially in connection with the security of personal data in the sense of Act No. 101/2000 Coll., on the protection of personal data and on the amendment of certain laws, in as amended (hereinafter referred to as "ZOOU") and Regulation (EU) No. 2016/679 of the European Parliament and of the Council, on the protection of natural persons in connection with the processing of personal data and on the free movement of such data and on the repeal of Directive 95/46/EC (hereinafter referred to as "**GDPR**").

1.2. The Directive further defines the rights and obligations of the Operator's employees, or other natural and legal persons participating in activities related to the processing of personal data.

2. DEFINITION OF BASIC TERMS

For the purposes of this internal directive:

personal data means all information about an identified or identifiable natural person;

a person identified or identifiable by the data subject to whom the personal data relate; an identifiable natural person is a natural person who can be directly or indirectly identified, in particular by reference to a certain identifier, for example a name, identification number, location data, network identifier or to one or more special elements of physical, physiological, genetic, psychological, economic, cultural or the social identity of this natural person;

sensitive personal data means any data on racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person and data on the state of health or on the sex life or sexual orientation of a natural person persons;

with the consent of the data subject, any free, specific, informed and unequivocal expression of will by which the data subject gives his consent to the processing of his personal data by means of a statement or other obvious confirmation;

processing of personal data means any operation or set of operations with personal data or sets of personal data which is carried out with or without the aid of automated procedures, such as collection, recording, arrangement, structuring, storage, adaptation or alteration, retrieval, inspection, use, disclosure by transmission , dissemination or any other disclosure, arrangement or combination, restriction, erasure or destruction;

an authorized person is any person who works with personal data in the framework of employment or cooperation with the Operator (regardless of whether it is a natural person - an employee or a so-called freelancer).

3. BASIC PRINCIPLES OF PERSONAL DATA PROCESSING

3.1. Only personal data obtained in a lawful manner may be processed.

3.2. Personal data can only be processed in cases stipulated by the General Regulation on the Protection of Personal Data, the ZOO and other legal regulations, while it is necessary to comply with the provisions of this Directive, as well as other related internal regulations of the Operator.

3.3. Personal data is stored only for the time necessary for the purpose of its processing. They must then be disposed of or anonymized.

3.4. The operator does not process sensitive personal data.

3.5. The operator does not perform any profiling or automated decision-making.

3.6. The Operator does not process personal data on the basis of consent (the reason for processing is always the law, contract or legitimate interests of the Operator, possibly another reason other than consent and the fulfillment of the rights and obligations of public entities).

4. OVERVIEW OF PROCESSING

4.1. The annex to this Directive forms a basic overview of the processing of personal data, including the entities concerned, the scope of processing and the processors used.

5. INSTRUCTIONS AND TRAINING

5.1. Before any authorized person is admitted to personal data, he must be made aware of the fact that he will work with personal data as part of his activity. The content of the training must be in particular the nature of the processes that include personal data, security principles and procedures according to this directive. The training must be certified by signing the protocol that the person has been informed of the obligations regarding the processing of personal data. The operator will regularly verify the fact that the authorized person follows the given instructions, especially in the form of additional training.

5.2. It is not possible for an authorized person to start working with personal data without appropriate training.

5.3. The authorized person is explicitly informed with which system he is authorized to work and what permissions he has in the system. The authorized person may not work with personal data in a system other than the one entrusted to him, even if he has actual access to such a system.

6. WORKING WITH PERSONAL DATA

6.1. Personal data is mainly contained in the Previo system. In the case of work in this system, it is forbidden to copy any data outside this system

.6.2. Authorized persons proceed in such a way that there is no duplication of data and personal data contained in the {Previo} system is not duplicated, e.g. on paper. If this is necessary, after entering the data in {Previo}, the authorized person is obliged to destroy the duplicate document.

6.3. It is forbidden to combine the data collected for different purposes - the {Previo} system is automated and in the area of reservations it performs the matching of data in accordance with their purposes.

6.4. The operator processes only true, accurate and updated personal data. For this purpose, authorized persons are obliged to verify the correctness and accuracy of personal data. If the correctness and accuracy of the personal data cannot be verified or it turns out that the personal data provided is not correct and accurate, the authorized person is obliged to correct or destroy the personal data without delay.

7. OBLIGATIONS FOR RESERVATIONS

7.1. The person in charge of processing reservations (in particular, the person in charge of managing the Operator's account within the reservation portals booking.com, expedia.ie, hrs.de, hotel.cz) is obliged to properly inform persons visiting the Operator's profile about the protection of personal data. The relevant text of this information is given to the authorized person. In case of an update, the

authorized person will be informed. The authorized person is not authorized to change the relevant text without the consent of the Operator.

7.2. The authorized person will communicate with interested parties through the Internet reservation portal - however, he will not copy the relevant communication into the {Previo} system.

8. OBLIGATIONS FOR ACCOMMODATION OF GUESTS

8.1. When registering guests to the accommodation, an approved document - privacy protection and information on the processing of personal data is submitted. Each guest must be able to familiarize himself with the given document and the reception staff must be prepared to provide the necessary assistance in the explanation. The document must be submitted in the following languages - Czech and English. Both language mutations must be available within each room or other accommodation space.

8.2. At the same time, the authorized person is obliged to identify persons based on the obligations under the Act on Foreigners and the Act on Local Fees and enter the relevant data into the {Previo} system and further into the relevant books kept in paper form.

9. PROTECTION OF WRITTEN DOCUMENTS

9.1. If personal data is contained in paper documents, these must be kept in a lockable place in lockable areas to which only a limited circle of authorized persons can access.

9.2. If personal data within documents can no longer be stored due to the end of the duration of the purpose of processing, the given document is shredded, unless they are documents that must be further archived according to special regulations.

9.3. On the access of authorized persons to documents containing personal data, records will be kept by the authorized person, designated for this purpose, containing at least the following data: designation of the document, name and surname of the person who worked with the document, details of when the document was submitted for processing and when it was returned, and signature of the authorized person to whom the records are entrusted.

9.4. It is forbidden to create any copies of documents, unless it is a necessary process - at the same time, it is forbidden to take any documents outside the Operator's premises.

10. PROTECTION OF ELECTRONIC RECORDS

10.1. Access to the *{Previo}* system is logged, so it is evident what changes have occurred in the system, for the purpose of possible data recovery.

10.2. The authorized person is entrusted with a login and password for access to the system, which he is obliged to protect and not disclose to anyone. The password must be changed regularly,

according to the system's instructions for changing the password. It is expressly forbidden to record the password and login on paper or other material, especially within direct reach of the possibility of accessing the *{Previo}* system.

10.3. After the end of the cooperation between the authorized person and the Operator, the person entrusted with IT administration is obliged to change the login data and passwords to which the authorized person had access.

11. CAMERA RECORDS

11.1. It is the responsibility of the authorized person to delete the records after 14 days from their acquisition. Camera recordings must not be copied outside the relevant storage on the Operator's hardware.

11.2. It is also the responsibility of the person in question to ensure that a notice with the appropriate pictogram is displayed in the monitored premises.

12. MEDIA AND HARDWARE

12.1. In the event that personal data is stored using media or other hardware, these, as well as written documents, must be stored in a lockable place in lockable rooms to which only a limited circle of authorized persons can access.

12.2. If personal data within the hardware and media can no longer be stored due to the end of the duration of the processing purpose, the given media or hardware is disposed of.

12.3. It is forbidden to create any reproductions of media or hardware, unless it is a necessary process - at the same time, it is forbidden to take any media or hardware outside the Operator's premises.

12.4. It is forbidden to store personal data on mobile or any other personal devices.

13. SECURITY OF PERSONAL DATA

13.1. The person entrusted with the management of the IT solution is obliged to propose to the management of the Operator such technical and organizational measures as to prevent unauthorized or accidental access to personal data, their change, destruction or loss, unauthorized transmission, their other unauthorized processing, as well as other misuse of personal data data. These measures must be reviewed regularly. Persons responsible for the IT area ensure obligations in the protection of personal data stored on servers, in personal computers, including portable ones, so that the protection of stored data is ensured in accordance with the current requirements for computer security and to maintain it in that state.

13.2. In the event that new technologies are to be deployed, or new method of processing, in order to deploy such technology, it is always necessary to first assess whether it is a suitable and safe technology for the processing of personal data. This assessment must be made in writing and must be accompanied by a technical and legal assessment of the application of such technology. Ensuring this assessment is the responsibility of the authorized IT person.

14. AUTHORIZED PERSONS

14.1. Authorized persons are persons who act on behalf of the Operator and are authorized to process personal data on the instructions of the Operator.

14.2. Personal data may be processed and accessed only by authorized persons who have this stated in their job description, and only under the conditions and to the extent set by this directive, exclusively within the scope of their work tasks. Specific authorized persons are listed at the end of this document.

14.3. The authorized person is obliged to act in such a way that unauthorized persons are not allowed to obtain processed personal data, e.g. by cleaning/shredding unused documents left on the table. For the same purpose, when leaving the workplace, the authorized person is obliged to clean up the workplace and log off or switch off the device he was working on. The authorized person is obliged to follow the "empty monitor, empty desk" rule.

14.4. Upon termination of cooperation between the authorized person and the Operator, the authorized person is obliged to hand over the keys to the lockable premises. Making copies of keys is prohibited.

14.5. Authorized persons are required to study and familiarize themselves with this Directive.

14.6. If the authorized person is a legal entity, or another person that uses third parties in the performance of tasks for the Operator or the provision of services, it is obliged to transfer all obligations arising from this directive to these third parties and oblige them to fulfill their obligations according to the protection of personal data.

14.7. Each senior authorized person is obliged at the subordinate workplace where personal data is processed, and for authorized persons subordinate to him:

a. regularly check whether personal data are processed in accordance with the stated purpose;

b. ensure the protection of personal data against unauthorized access, processing, or misuse of information;

c. to determine the means and method of information processing as part of ensuring information protection;

d. ensure the processing of only true and accurate personal data (verify the processed data), and only to the extent necessary to fulfill the specified purpose;

e. ensure the retention of personal data only for a period that is necessary for the purpose of their processing or that is stipulated by a special law.

15. PROCESSOR ENGAGEMENT

15.1. For the processing of personal data, the operator uses only processors who provide sufficient guarantees for the introduction of appropriate technical and organizational measures so that the processing meets the requirements of legal regulations and to ensure the protection of the data subject's rights.

15.2. The involvement of the processor is approved by the management of the Operator after consultation with an authorized person in the field of IT and a possible legal opinion as to whether it is a satisfactory solution.

16. OPERATOR AS PROCESSOR

16.1. In the event that the Operator is a processor of personal data for another person, e.g. if it allows the use of its reception capacities, software, IT consultancy for another accommodation provider, all persons entrusted with data processing must consistently distinguish whether it is the personal data of the Operator or other persons. In relation to this data, they must perform all obligations regarding their protection as if it were the Operator's data. The person entrusted with the management of this data then issues binding instructions on how this data should be handled, especially at the end of the processing. The authorized person's binding instructions must be in accordance with the processing contract, the provisions of which take precedence over this directive. In the event of a conflict, the management of the Operator decides.

17. EXERCISE OF RIGHTS

17.1. The operator enables data subjects to request access to their data and exercise their rights under the GDPR through the web interface. These requests come via email. Iva Ledererová is the person authorized to handle them.

17.2. On the basis of this request, the authorized person will notify the management of the Operator in writing and, in cooperation with the person authorized for IT, if necessary. after legal consultation, they will provide the applicant with the necessary information in terms of his request. The content of the response is approved by the management of the Operator.

17.3. This process must be processed without delay, no later than 1 month after receipt. The authorized person for this process is obliged to register this deadline.

17.4. The same procedure is followed if the request is made by another data subject.

18. REPORTING TO THE AUTHORITY

18.1. In the event that any authorized person discovers a breach of personal data security, they are obliged to inform the authorized person for IT and the management of the Operator about this without undue delay. These persons must assess without undue delay whether the breach is unlikely to result in a risk to the rights and freedoms of natural persons. If this is not the case, the authorized person (management of the Operator) is obliged to report this violation (including other facts in the form) to the Office for Personal Data Protection on the appropriate form. This notification must be made without undue delay, at the latest within 72 hours, from the moment the first authorized person became aware of it.

18.2. If it is likely that a certain case of personal data security breach will result in a high risk for the rights and freedoms of natural persons, the Operator will notify the data subject of this breach without undue delay.

18.3. In the case of processing in the position of a processor, the authorized person for the management of the Operator will notify the relevant administrator.

19. DISPOSAL OF PERSONAL DATA

19.1. As soon as the purpose for which the personal data was processed no longer exists, or based on the data subject's request (if justified), the Operator will dispose of the personal data, in particular in the following manner:

a. shredding original documents;

b. deleting personal data in electronic databases;

c. disposal of media and other hardware containing personal data

d. anonymization (i.e. deletion of name, surname and residential address);

e. permanent exclusion from further processing.

19.2. Liquidation will be carried out for personal data depending on the deadlines for their processing

a. Personal data processed for the purpose of accommodation will be processed for the entire time that the accommodation lasts and then for a period of 6 months from the end of the accommodation for the purpose of possible complaints. Name, surname and address of residence and communication will be kept by the Operator for a period of 3 years from the end of accommodation for the purpose of recording any claims in legal disputes.

b. Personal data processed for the purpose of registering foreigners will be processed in accordance with the Act on the Residence of Foreigners for a period of 6 years from the last entry in the house book, or for a period of 6 years from the end of the accommodation of the accommodated person.

c. Personal data processed according to the Act on Local Fees will be processed for a period of 6 years from the last entry in the register.

d. The processing time for accounting documents is 5 years from the end of the accounting period, in the case of documents relevant for VAT payments, it is 10 years from the end of the tax period in which the performance took place.

e. identification data and email for the purpose of sending commercial messages about services until the time when cancellation is requested,

f. Camera recording for 14 days.

g. Personal data of suppliers for the duration of the performance of the contract and subsequently for the duration of the applicable limitation periods for claiming compensation for damages, or registration of copyrights.

20. AUTHORIZED PERSONS

List of authorized persons:

IT security and technology (including hardware and its disposal) - IT administration	Amccomp, s.r.o.
Approval of documents in the field of personal data protection	Kamila Rousová
Reception service	Kamila Rousová
Operation of the booking portal booking.com	Kamila Rousová
Operation of the reservation portal hrs.de, expedia, hotel.cz	Kamila Rousová
Document shredding	Kamila Rousová
Camera systems	Kamila Rousová
Accountancy	Rudolf Novosad
Approval of procedures differing from this directive	Kamila Rousová
Handling client requests according to GDPR	Kamila Rousová
Management of the Operator responsible for the area of personal data	Kamila Rousová

21. REVISION OF DIRECTIVE

21.1. The revision of this Directive is carried out if necessary, but at least once every 2 years. Kamila Rousová is responsible for the processing, enforcement, maintenance and revision of the Directive for handling personal data

22. EFFECTIVITY OF DIRECTIVE

22.1. This Directive becomes valid and effective on 25/05/2018

Brno _____

_____

Kamila Rousová