Privacy Policy
CFR Kft.
Hotel Flanders
Enters into force: 16.02.2024.
(The regulation is valid together with its annexes.)

CFR Kft. the Hotel Flandria community accommodation (address: 27. Szegedi út Budapest 1135; website: www.hotelflandria.hu) as the operator and undertakes obligations as a data manager that all data processing related to its activities complies with this information and in the applicable national legislation, as well as in the legal acts of the European Union specific expectations.

CFR Kft. manages the personal data that the

- employees,
- Flandria Hotel guests or future guests,
- its contracted partners (e.g. tenants, services to be performed in its territory, e.g.: asset protection, cleaning, maintenance, renovation, etc. companies performing activities employees)

are made available, respectively

other persons whose names and data (e.g. emergency responder colleague, police, fire department, control authorities, other business partners, etc.) are recorded during the Flandria Hotel's business process.

The purpose of this information is that natural persons belonging to the categories listed above their data can receive appropriate information before entering their personal data on the purpose, legal basis of its processing, scope and deadline of the processed data.

Data and contact details of the Data Controller:

Name of the data management company:	CFR Gazdasági Tanácsadó Kft.
Abbreviated company name:	CFR Kft.
Headquarters and postal address:	27. Szegedi út Budapest 1135
Company registration number:	Cg.01-09-561306
Representative and data protection officer:	Managing Director Tibor Németh
His phone number is	+36 1 350 3181
E-mail address:	info@hotelflandria.hu

(hereinafter also referred to as "Data Controller" or "Company" or "Hotel Flandria")

Data Protection Officer:

Name of the data protection officer**:**	Norbert Balázs dr.
Contact:	info@hotelflandria.hu

The Privacy Policy must be posted in printed form by the Flandria Hotel at the reception and on the hotel's website (www.hotelflandria.hu).

Interest assessment test: The Data Controller performed the interest assessment test, during which established that the legitimate interests of the data controller take precedence over the interests of the data subjects, against your personal rights.

Data protection guidelines applied by the Data Controller

Hotel Flandria is committed to protecting the personal data of its customers and partners,
and considers it of paramount importance to respect the right of its customers to information self-determination.
The Company treats personal data confidentially and takes all security,
technical and organizational measures that guarantee the security of the data.
The Data Controller uses personal data on the basis of the legal basis set out in the GDPR and exclusively for the specified purpose.
Personal data may be processed exclusively for a specific purpose. At every stage of data processing, it must comply with the purpose of data processing, and the collection and processing of data must be fair and lawful.
Only personal data may be processed that is indispensable for the achievement of the purpose of data processing and is suitable for achieving the purpose. Personal data may only be processed to the extent and for the period necessary for the achievement of the purpose.
The Data Controller shall not use personal data for purposes other than the specified purposes.
In all cases where the Data Controller intends to use the provided personal data for a purpose other than the original purpose of data collection, it shall inform the Data Subject thereof and obtain his/her prior, express consent, or provide him/her with the opportunity to prohibit the use of his/her personal data. Our data management principles are in accordance with the applicable data protection legislation, which are set out in Annex 1.

TERMS USED IN THE NOTICE

Data subject: According to the GDPR, “data subjects” are natural persons residing anywhere in the EU who are in contact with a “data controller” or natural persons residing in the EU who are in contact with a data controller outside the EU.
Data controller: the legal entity that determines the purposes and means of the processing of personal data.
Personal data: any information relating to an identified or identifiable natural person (“data subject”).
An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, a number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Data management: any operation or set of operations which is performed on personal data or on data files, whether or not by automated means, such as collection, recording, structuring, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Data processor: the legal entity which processes personal data on behalf of the controller.

Data processing: the performance of technical tasks relating to data processing operations, regardless of the method and means used to carry out the operations and the place of application, provided that the technical task is carried out on the data.
Consent of the data subject: any freely given, specific and informed and unambiguous indication of the data subject's wishes by which the data subject indicates that the data subject's statement or confirms that he/she consents to the processing of personal data concerning him/her by means of a clear and unambiguous confirmation.
Data erasure: the making of data unrecognizable in such a way that their recovery is no longer possible.
Profiling: any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal characteristics relating to a natural person, in particular to analyse or predict characteristics relating to his/her performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
Pseudonymisation: The encoding or other maintenance of personal data in such a way that they cannot be attributed to a specific data subject without providing additional information. The additional information must be stored separately and protected against unauthorised use by means of technical and organisational measures.
Third party: a natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor or the persons who, under the direct control of the controller or processor, are authorised to process personal data.
Third country: any State which is not a member of the European Economic Area (EEA)

PREAMBLE

Hotel Flandria operates as a community accommodation, primarily as employee accommodation.
Its clients are mainly business companies that provide accommodation for their employees for a longer period of time.
This also means that Hotel Flandria does not, as a matter of practice, accept individual private guests.
Accommodation can only be booked by email, telephone or in person.
Accommodation can be used in the form of a rental or accommodation service.
Hotel Flandria also utilises other areas in the form of long or medium-term rental structures (e.g. warehouse, parking).
To provide the services, CFR Kft. partly uses its own employees and partly uses the help of service companies.
With regard to the employees of CFR Kft., detailed information regarding the GDPR is provided to the individual employees in the employment contracts and their supplements.

With regard to those business companies that provide services to CFR Kft., during which CFR Kft.
- employees,
- guests or prospective guests of Flandria Hotel,
- contracted partners (e.g. tenants, employees of companies performing services in its area, e.g.: asset security, cleaning, maintenance, renovation, etc.),

- other persons whose names and data (e.g.: emergency service employee, police, fire department, inspection authorities, etc.)

are in the possession of the service provider, CFR Kft. requires that service providers comply with the GDPR regulations in force at all times.

We provide the following information on the data processing carried out during certain services of Hotel Flandria:

1. ACCOMMODATION RESERVATION

In the case of a room reservation made by e-mail, in person at the hotel, or by telephone, our Company may request any or all of the personal data listed under "scope of processed personal data".

The purpose of data processing: the identification of the guest booking the room at check-in and the registration of the payment method, which can avoid the financial risk if the guest does not check in to the hotel.
The legal basis for data processing: the prior consent of the person booking the accommodation (Article 6
(1) (a) of the GDPR) and the necessity to take steps at the request of the person concerned before concluding a contract between the Data Controller and the Data Subject (Article 6
(1) (b) of the GDPR).
The scope of personal data processed includes: last name, first name, address (country, zip code, city, street, house number), date of arrival, date of departure, payment method: bank account number or full credit card details, telephone number, e-mail address.

Other preferences (e.g. payment method and frequency, etc.) in the case of third-country nationals, in addition to the above: border crossing location, time, visa number.

Data processing method: The commissioning partners primarily send the guests' data to the hotel's electronic mailing address. info@hotelflandria.hu.
This data may only be processed by designated employees of CFR Ltd. who are authorized to do so in their job descriptions and have participated in annual training in relation to the relevant legal norms in force.
This closed mailing system, managed only by employees of CFR Ltd., is continuously protected by our company with the most advanced security programs of the time and period during quarterly audits.

The data received at this address is transferred to a hotel registration program running on a separate computer without an internet connection (but how?), which enables the data provision and invoicing required by legal norms.

2. REPORT FORM

Purpose of data processing: realization of accommodation reservation, recording of data required by law

Legal basis for data processing: data processing is necessary to take steps at the request of the data subject prior to concluding a contract (GDPR Article 6 (1) point b)), and
data processing is necessary to fulfill a legal obligation to the data controller (GDPR Article 6 (1) point c))
Scope of personal data processed: Surname, first name, date of birth, ID card number/Passport number, residential address/billing address, e-mail address, payment method, arrival and departure date, vehicle registration number.
Duration of data processing: Data processed for the purpose of providing services are stored for 2-8 years, depending on the data, in order to comply with the related legal standards.
In some cases, there is an obligation to store personal data for a longer period prescribed by law. Such cases include:
• If the data is required for issuing an invoice or other tax records, the data must be retained for 8 years from the end of the calendar year.
• The hotel must pay tourist tax to the local government for guests using the accommodation service in accordance with the applicable laws, and guests arriving from outside the EU must be reported to the police. The statutory retention period for the data recorded in these reports is 6 years from the date of check-in.
If you expressly request that your data be retained in order to simplify future bookings (data processing purpose), the legal basis for data processing will be your voluntary consent.
You may withdraw your consent at any time, but the withdrawal will not affect previous lawful data processing. We will delete the data after the longest of the relevant data retention periods mentioned. The provision of mandatory data by the Guest is a condition for using the hotel service.

Data management method:
For guests who fill out a form by hand upon check-in, the data from the completed forms is transferred to a hotel registry program run on a separate computer that does not have an internet connection by the person performing the work processes at the reception, which also enables the data provision and invoicing required by legal norms.

After that, the manually filled out forms are placed separately in a locked cabinet in the company management's closed office until the end of the retention period specified in the legal norms, and then they are destroyed by "crushing" them, making recovery impossible.

3. CAMERA SYSTEM

There are cameras operating in the Hotel Flandria area for the personal and property safety of employees, guests and tenants. The persons performing tasks at the reception are entitled to view the images of the cameras on the monitors placed there, and the recordings are recorded.

The camera surveillance is indicated by the relevant pictogram and warning text in Hungarian and English at the entry points of the area.

The purpose of data processing: to protect the life and physical integrity of persons staying in the Hotel Flandria area, to maintain personal and property safety by using the electronic surveillance system (camera system).
With special attention to the protection of human life, especially against man-made disasters (e.g. fire, prevention of mass danger) and in order to detect and take action as soon as possible.
The use of cameras is justified by the fact that there have been several cases of personal injury and property damage caused by accidents and intentional acts by other people and by oneself in the accommodation area.
An additional reason is that recording the images of the cameras allows for the collection of evidence related to civil law claims.
The images transmitted by the cameras allow for immediate action, and the recording of the images helps to reconstruct the events later, which can lead to the detection of the perpetrators of the violations, compensation for damages in the interests of the victims, and the enforcement of society's criminal law claims.

There is no secondary intention to use the camera images. For example: marketing, employee performance monitoring, etc.
The data controller does not process biometric data. The system is not suitable for facial recognition, face recognition or analysis.
The use of the camera system is necessary and justified, taking into account the size of the building and the area belonging to it, the general number of people accommodated in it, so the underlying goal cannot be reasonably achieved by other means, despite the fact that other means are also used in combination.
Considering that the work and rest schedule of the accommodated guests varies, and based on their rhythm of life, their movement is constant 24 hours a day, so the possibility of accidents causing personal injury and man-made disasters (e.g. fire) exists 24 hours a day, the camera system is therefore operated 24 hours a day.
The images transmitted and recorded by the camera system take place exclusively within the data controller's property and do not look out onto public areas or neighboring properties. When making the decision on the operation of the camera system, we took into account the principle of balancing interests, based on which it can be clearly established that the immediate detection of disasters caused by man or by accident, the taking of measures, the detection and interruption of violations of rights are more important than the rights and interests of the data subjects.
When considering the principle of reasonable expectations of data subjects, we took into account the provisions of the Guidelines, according to which data subjects can expect not to be observed in lounges, parks, and kitchens, but we also established that the immediate detection of disasters caused by man or by accident, the taking of measures, the detection and interruption of violations of rights are more important than the rights and interests of the data subjects.
The legal basis for data processing is the explicit voluntary consent of the Data Subject [Article 6 (1) point a) of the GDPR], point d) of the same norm (data processing is necessary to protect the vital interests of the Data Subject or another natural person), and the legitimate interests of the Data Controller pursuant to the provisions of Section 26 (1) point e) and Section 31 (1) of the Szvtv [Article 6 (1) point f) of the GDPR].

The scope of personal data processed: the facial image and behaviour of the Data Subjects as seen in images. No audio recording is made.

Duration of data processing: the maximum period specified in the legal norms in force from the time the Data Subject enters the Hotel Flandria area.

Data management method: images transmitted by cameras can be viewed by the persons performing work tasks there through monitors placed at the reception, who monitor the images transmitted by the cameras as part of their tasks and take action if necessary.

The recordings are recorded and stored on a separate server that does not have an internet connection.
The recordings can only be accessed by entering a password.
The separate server storing the recordings is located in a physically protected location.

If it is necessary to review the recordings recorded by the cameras, only designated persons may review them, and they must then record the reason for this, the duration of the viewed recordings, and the events in the register set up for this purpose, including the investigation of any fire or accident incidents, during which the recording relating to the specific event may also be viewed by the fire and occupational safety specialist. (The contact details of the fire and occupational safety officer are included in Appendix 2.)

If it is necessary to copy the recorded recordings (e.g. for use as evidence in proceedings conducted by an investigative authority), the designated person shall save them on a data carrier during the review, and then record the reason for this, the duration of the viewed and copied recordings, and the events in the register set up for this purpose.

If the saved recordings must be temporarily kept by the Company, they shall be placed in a closed office, in a locked cabinet, inaccessible to unauthorized persons, and in a room monitored 24 hours a day.

If the recorded recordings are not copied, the system will delete them automatically, without human intervention, and irretrievably at the latest time specified in the legal norm in force at all times, according to the rules applicable to us.

The cameras do not overlook public areas, they only monitor the area owned by the company.

4. COMMUNITY PORTALS

Hotel Flandria is available on the Facebook community portal.

Purpose of data processing: new information, news, current events about the hotel, possible, occasional contact.

Legal basis for data processing: the data subject's voluntary consent (GDPR Article 6 (1) (a) point).
Consent can be withdrawn at any time by unsubscribing. The withdrawal does not affect the previous lawful data processing. In the event of withdrawal, you will not receive a notification about our news feed, our news will not appear on the person's news feed, but you will still have access to the news feed, as our page is public.

Scope of personal data processed: The Company has access to the profiles of "followers", but does not record them and does not manage them in its own internal system.
Duration of data processing: data processing lasts until the individual unsubscribes.
The Company also publishes pictures/films about various events/hotels, etc. on its Facebook page.
Unless it is a mass recording, the Company always requests the written consent of the data subject before publishing the images.

Facebook is an independent data controller from us. You can find information about the data processing of the page in the data protection guidelines and regulations on the Facebook website.

5. AUTOMATICALLY RECORDED DATA, COOKIES

When you visit our website, the following data from your device are automatically recorded.

- name,
- e-mail address.

The data recorded is automatically logged by the web server serving the website without your separate declaration or action while you are visiting the website.
The system automatically generates statistical data from this data.
The collected data cannot be linked to other personal data, except in cases required by law.
We use this information exclusively in a summarized and processed (aggregated) form, in order to correct any errors in our services, improve their quality and for statistical purposes.

The purpose of data management: Technical development of the IT system, monitoring the operation of the service and preparing statistics. In case of abuse, the data can also be used to establish the source of the abuse in cooperation with the visitors' internet service provider and the authorities.
Legal basis for data processing: The condition for the provision of the service pursuant to Section 13/A. (3) of Act CVIII of 2001 on electronic commerce services and certain issues related to information society services.
Duration of data processing: 5 days from the date of viewing the website.
Cookies and similar technologies

What is a cookie?
A cookie is a small text file that is stored on the hard drive of a computer or mobile device for the expiration period set in the cookie and is activated (returned to the web server) on subsequent visits. Websites use cookies to record information about the visit (pages visited, time spent on the pages, browsing data, exits, etc.) and personal settings,

however, this is data that cannot be linked to the person of the visitor. This tool helps to create a user-friendly website to enhance the online experience of visitors.

On other platforms – where cookies are not available or cannot be used – other technologies may be used, the purpose of which is similar to that of cookies: for example, the advertising identifier on Android mobile devices.

There are two types of cookies: “session cookies” and “persistent cookies”.
• “Session cookies” are stored by your computer, notebook or mobile device only temporarily, until you leave the website; these cookies help the system to remember information, so that you do not have to repeatedly enter or fill in the information. The validity period of session cookies is limited to the user’s current session, and their purpose is to prevent data loss (for example, when filling out a long form). Once the session ends or the browser is closed, this type of cookie is automatically deleted from the visitor's computer.
• “Persistent cookies” are stored on the computer, notebook or mobile device even after leaving the website. With the help of these cookies, the website recognizes you as a returning visitor. Persistent cookies are suitable for identifying you through the server-side identifier-user association, thus in all cases where user authentication is essential - e.g. web shop, netbank, webmail - a necessary condition for correct operation. Persistent cookies do not carry personal data by themselves and are only suitable for identifying the user together with the association stored in the server's database. The risk of such cookies is that they do not actually identify the user, but the browser, i.e. if someone is in a public place, e.g. If you enter a web store in an internet café or library and do not log out when you leave, another person can later use the same computer to access the web store in the name of the original user.

How can you enable or disable cookies? Most web browsers automatically accept cookies, but visitors can delete or refuse them. Since each browser is different, you can set your cookie preferences individually using your browser's toolbar. If you do not want to allow any cookies from our website, you can change your web browser settings to notify you when cookies are sent, or simply refuse all cookies. You can also delete cookies stored on your computer or mobile device at any time. For more information about settings, see your browser's Help. Please note that if you choose to disable cookies, you will have to give up certain features of the website.

What cookies do we use?

1. Tools essential for the operation of the website:
Such cookies are essential for the proper operation of the website, so in this case
the legal basis for data processing is Act CVIII of 2001 on electronic commerce services and certain issues of information society services, § 13/A. (3) paragraph. No data transfer takes place.

a) Helps with searching
Purpose of data processing: Helps with searching so that you can find what you are looking for as quickly as possible.
Data processing time: lasts for the duration of your stay on the website

b) Identifying language settings:
Purpose of data processing: During your visit to the website, the system uses a standard cookie to identify you as a unique user in order to remember your language settings.
Data processing time: This setting (cookie) is stored for 5 days.

c) Social network cookie (Facebook)
In this regard, Facebook, as a service provider independent of us, acts and provides information on its own website.

6. REFERENCES AND LINKS

Our website may also contain links that are not operated by the Company, but only serve to inform visitors. The Company has no influence whatsoever on the content and security of websites operated by partner companies, and is therefore not liable for them. Please review the data management information of the websites you visit before providing your data in any form on the given website.

7. BILLING

Purpose of data management: Use of services provided by Hotel Flandria, determination of the price of the services and invoicing.
Legal basis for data management: Section 69 of Act C of 2000 on Accounting. (1) and (2) (GDPR Article 6 (1) (c)).
Scope of personal data processed: Company name, billing address or business address provided for the issuance of the invoice, duration of stay (arrival-departure date), tax number. In the case of other organizations, sole proprietorships, other legal forms, the name specified in the law.
Duration of data processing: 8 years from the date of provision of personal data by the data subject and the preparation of the report, business report or accounting settlement for the given business year.
Possible consequences of failure to provide data: The data subject may not use the services of Hotel Flandria.
The performance certificates required for the issuance of invoices do not contain data regarding guests.

8. COMPLAINT HANDLING LOG

During the handling of consumer complaints, if you do not agree with the handling of the complaint or if the complaint is not immediately investigated, the Company is obliged to immediately record the complaint and its position on it.
The log contains the following data:
• Name, address or registered office of the complainant,
• Place, time and method of submitting the complaint
• Detailed description of the complaint, list of documents and other evidence presented by the complainant

• Statement of the Company on its position on the consumer's complaint, if the complaint is immediately investigated
except for the complaint - the signature of the complainant
• Place and time of recording the log
• In the case of a complaint submitted by telephone or electronically, the unique identification number of the complaint

Purpose of data processing: investigation of the complaint and maintaining contact with the complainant.

The legal basis for data management is: Section 17/A. (7) of Act CLV of 1997 on Consumer Protection, which makes the above data management mandatory.

Duration of data management: 5 years from the date of recording the minutes.

If you wish to exercise any of your rights set out in this data protection notice in relation to the data provided in this way, or wish to contact us for any other reason in relation to the above data management, please notify us by letter sent to 1135 Budapest, Szegedi út 27.
or by e-mail sent to info@hotelflandria.hu.

9. CONTACT

You have the opportunity to contact us via any of our contact details
(Telephone, e-mail, by post, in person). In such a case, we assume your consent to the processing of the data shared with us.

The purpose of data management is: to answer questions and requests, to maintain contact with the applicant.
The legal basis for data processing is the voluntary consent of the data subject (Article 6 (1) (a) of the GDPR). Consent may be withdrawn at any time. The withdrawal does not affect the lawful processing of data prior to it.
Scope of personal data processed: we request the most necessary data to answer the given question.
Duration of data processing: after answering the given request, question or complaint, we delete the personal data received after the maximum period of the possibility of initiating civil litigation, determined on the basis of the applicable legal norm.
However, if it is necessary due to the nature of the correspondence - for tax or accounting reasons, or perhaps to protect the rights and interests of the Company or the applicant, we archive it and - in each case individually examined - store it for the necessary period.

10. BUSINESS RELATIONSHIP

Like most companies, our Company also maintains business relationships with some employees of other organizations, whose names, business positions and contact details are stored.

Purpose of data processing: communication with our partners for the purpose of cooperation.

Legal basis for data processing: Legitimate interest in the performance of the contract or in maintaining relations between companies (GDPR Article 6 (1) (f)).
Scope of personal data processed: name, business position, telephone number,
e-mail address of the contact person.
We store the contact details of these business contacts solely for the purpose of facilitating the establishment and maintenance of business cooperation with partner companies.

Duration of data processing: we check the contact details of our business contacts at least annually and remove those that are no longer relevant from the system.
At the request of the partner, we modify or remove their data from our system.

We proceed in the same way as above when processing the personal data of press representatives.

OTHER DATA PROCESSING

We will provide information on data processing not listed in this information when collecting the data. We inform our customers that certain authorities, bodies performing public tasks, and courts may contact our company for the purpose of disclosing personal data. Our company will only provide these bodies with personal data - if the body concerned has indicated the exact purpose and scope of the data - to the extent that it is absolutely necessary to achieve the purpose of the request and if the fulfilment of the request is required by law.

11. TRANSFER OF DATA, INVOLVEMENT OF DATA PROCESSORS

Our company partially uses the assistance of IT service providers according to the following:

Name, registered office, description of tasks of the data processor
see. No. 2 Annex

Name of the company that performs payroll accounting for our employees:
see. Annex 2

Name of the company that performs the accounting tasks of the Company:
see. Annex 2

Name of the company that performs the tasks of the fire and occupational safety officer:
see. Annex 2

Our Company, as the Data Controller, is entitled and obliged to forward all personal data at its disposal and duly stored by it to the competent authorities, which it is obliged to forward by law or a legally binding official obligation. The Data Controller cannot be held liable for the forwarding of such data and the consequences arising therefrom.

The Data Controller shall only carry out the transfer of data not indicated above with the prior and informed consent of the Interested Party.

12. METHOD OF STORAGE OF PERSONAL DATA, SECURITY OF DATA PROCESSING

Our company's IT systems and other data storage locations are located at the headquarters and at its data processors.

We select and operate the IT tools used to process personal data during the provision of the service in such a way that the processed data:
a) is accessible to those authorized to do so (availability),
b) its authenticity and authentication are ensured (authenticity of data processing),
c) its unchangeability can be verified (data integrity),
d) is protected against unauthorized access (data confidentiality).

We pay particular attention to data security, and we also take the technical and organizational measures and develop the procedural rules that are necessary to enforce the guarantees under the GDPR.
We protect the data with appropriate measures, in particular against unauthorized access, alteration, transmission, disclosure, deletion or destruction, as well as accidental destruction, damage, and inaccessibility due to changes in the technology used.
Our company's IT system and network are protected against computer-aided fraud, computer viruses, computer intrusions and denial-of-service attacks.
The operator also ensures security with server-level and application-level protection procedures.
Data backup is provided.

In order to avoid data protection incidents, our company takes all possible measures, and in the event of such an incident, we take immediate action to minimize the risks and prevent damage.
Electronic messages transmitted over the Internet, regardless of the protocol (e-mail, web, etc.), are vulnerable to network threats that may lead to dishonest activity or disclosure or modification of information.
The Company takes all reasonable precautions to protect itself from such threats. However, the Internet is not 100% secure, as is well known to users.
The Company is not liable for any damage caused by unavoidable attacks that may occur despite the greatest possible care.

13. RIGHTS OF THE DATA SUBJECTS

Right to information:

The controller shall take appropriate measures to provide the data subjects with all the information referred to in Articles 13 and 14 of the GDPR and all the information referred to in Articles 15 to 22 and 34 in a concise, transparent, intelligible and easily accessible form, in clear and plain language, and in a precise manner.

The right to information may be exercised in writing, via the contact details provided under “Data controller details and contact details”.

The data subject may also be provided with information orally upon request – after verification of his or her identity. We inform our clients that if our company’s employees have doubts about the identity of the data subject, we may request the provision of the information necessary to confirm the identity of the data subject.

Right of access:

The Data Subject has the right to receive feedback from the Data Controller as to whether his or her personal data is being processed, and if such processing is taking place, he or she has the right to access the personal data and the following information:

• The purposes of the processing in relation to the personal data in question,

• The categories of personal data concerned,

• The categories of recipients to whom the Data Subject's personal data have been or will be disclosed, including in particular recipients in third countries (outside the European Union) or international organisations,

• The planned period for which the personal data will be stored,

• The rights of the Data Subject (right to rectification, erasure or restriction, right to data portability and right to object to the processing of such personal data),

• The right to lodge a complaint with a supervisory authority,

• If the data is not processed by the Data Controller obtained from the Data Subject, then all available information regarding the source,

• the fact of automated decision-making concerning the Data Subject's personal data, including profiling, as well as understandable information about the logic involved and the significance of such data processing and the expected consequences for the Data Subject.

(Our company does not use automated decision-making and does not carry out profiling.)

If the Data Subject submitted his request electronically, the requested information shall be provided in a widely used electronic format, unless the Data Subject requests otherwise.

The Data Controller may request the Data Subject to specify its content and to specify the requested information and data processing activities before fulfilling the request.

If the Data Subject's right of access under this section adversely affects the rights and freedoms of others, in particular the business secrets or intellectual property of others, the Data Controller shall be entitled to refuse to comply with the Data Subject's request to the extent necessary and proportionate.

In the event that the Data Subject requests the above information in multiple copies, the Data Controller shall be entitled to charge a fee proportionate to the administrative costs of preparing the additional copies and at a reasonable rate. If the Data Controller does not process the

personal data indicated by the Data Subject, it shall also be obliged to inform the Data Subject in writing.

Right to rectification

The Data Subject shall have the right to request the rectification of the personal data concerning him/her.

If the personal data concerning the Data Subject are incomplete, the Data Subject shall have the right to request the completion of the personal data.

When exercising the right to rectification/completion, the Data Subject shall be obliged to indicate which data are inaccurate or incomplete and shall also inform the Data Controller of the accurate and complete data.

The Data Controller is entitled, in justified cases, to call on the Data Subject to provide the Data Controller with appropriate proof of the corrected data, primarily by means of a document.

The Data Controller shall correct and supplement the data without undue delay.

Right to erasure (‘right to be forgotten’)

The Data Subject shall have the right to request that the Data Controller erase personal data concerning him or her without undue delay where one of the following grounds applies:

• the personal data indicated by the Data Subject are no longer necessary for the purposes for which the Data Controller collected or otherwise processed them,

• the Data Subject withdraws his or her consent on which the processing is based and there is no other legal basis for the processing,

• the Data Subject objects to the processing based on the legitimate interests of the Data Controller and there are no compelling legitimate grounds for the Data Controller which override the interests, rights and freedoms of the Data Subject or for the establishment, exercise or defence of legal claims,

• the Data Controller has unlawfully processed the personal data,

• the Data Controller is required to process the personal data for a legal obligation to which the Data Controller is subject under Union or national law applicable to the Data Controller to fulfil the right to erasure,

• the Data Subject objects to the data processing and there are no overriding reasons for the data processing.

If the Data Controller grants the Data Subject's request for erasure, the Data Controller shall erase the processed personal data from all its records and shall inform the Data Subject accordingly.

After fulfilling the Data Subject's request to exercise the right to erasure, the Data Controller shall immediately inform the persons to whom the Data Subject has communicated his/her personal data, provided that this is not impossible or does not require a disproportionate effort

from the Data Controller. Upon the Data Subject's request, the Data Controller shall inform the Data Subject of these recipients.

The Data Controller is not obliged to delete personal data if the data processing is necessary:

• for the exercise of freedom of expression and the right to information,

• for the fulfilment of an obligation to process personal data imposed on the Data Controller by Hungarian or European Union law,

• for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller,

• for the implementation of public interests in the field of public health,

• for archiving purposes in the public interest, scientific and historical research purposes or statistical purposes, provided that the data processing would likely become impossible or seriously compromised as a result of the Data Subject's exercise of the right to be forgotten

• for the establishment, exercise or defence of legal claims.

Right to restriction of data processing:

The Data Subject has the right to request that the Data Controller restrict the processing and use of personal data concerning him or her, if one of the following reasons applies:

• the Data Subject disputes the accuracy of the personal data (in this case, the restriction shall last until the Data Controller verifies the accuracy of the data),

• the Data Controller has unlawfully processed the personal data, but the Data Subject requests restriction instead of deletion,

• the Data Controller no longer has the purpose of the data processing, but the Data Subject requires it for the establishment, exercise or defence of legal claims,

• the Data Subject objects to the data processing based on the legitimate interests of the Data Controller and there are no compelling legitimate grounds for the Data Controller which override the interests, rights and freedoms of the Data Subject or which are related to the establishment, exercise or defence of legal claims; in this case, the restriction shall apply until it is established whether the legitimate grounds of the Data Controller override those of the Data Subject.

In the event of restriction, personal data, with the exception of storage, may only be processed with the consent of the Data Subject, 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 important public interest reasons in the EU or a Member State of the European Union.

The Data Controller shall inform the Data Subject in advance of the lifting of the restriction on data processing.

Right to object:

In the case of a Data Controller, the right to object may arise in the case of data processing based on legitimate interest.

The Data Subject has the right to object to the processing of his or her personal data and in such a case the Data Controller may no longer process the Data Subject's personal data, unless it can be demonstrated that:

• the data processing is justified by compelling legitimate grounds on the part of the Data Controller which override the interests, rights and freedoms of the data subject or

• the data processing is related to the establishment, exercise or defense of legal claims of the Data Controller.

Right to object in the case of direct marketing:

Our company does not carry out direct marketing activities.

Automated decision-making in individual cases, including profiling:

Our company does not use automated decision-making, does not carry out profiling.

Right to data portability:

The Data Subject has the right to receive the personal data concerning him or her, which are processed by the Data Controller, in a structured, commonly used and machine-readable format and has the right to transmit those data to another data controller without hindrance from the Data Controller.

The right to data portability can be exercised in relation to personal data, which the Data Subject has provided to the Data Controller, and

• the processing is based on the Data Subject's consent or a contractual legal basis, and

• the processing is carried out by automated means.

If otherwise technically feasible, the Data Controller shall, at the Data Subject's request, transmit the personal data directly to another data controller, specified in the Data Subject's request.

In the context of data portability, the Data Controller is obliged to provide the Data Subject with the data carrier free of charge.

In the event that the Data Controller's right to data portability adversely affects the rights and freedoms of others, in particular the business secrets or intellectual property of others, the Data Controller is entitled to refuse to comply with the Data Subject's request to the extent necessary.

The measure taken in the context of data portability does not constitute the deletion of the data; the Data Controller will keep them as long as the Data Controller has an appropriate purpose or legal basis for processing the data.

Right of withdrawal:

The data subject has the right to withdraw his or her consent at any time. The withdrawal of consent does not affect the lawfulness of the data processing based on consent prior to its withdrawal.

Right to a remedy:

1. Right to lodge a complaint

If the Data Subject considers that the processing of his or her personal data by the Data Controller violates the data protection legislation in force at all times, in particular the provisions of the GDPR, he or she may lodge a complaint with the Data Protection Supervisory Authority.

If you do not normally reside in Hungary, but in another EU Member State, you have the right to lodge a complaint with the Supervisory Authority of the country concerned. You can find the names and contact details of the data protection authorities at the following link:

http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm

If you normally reside in Hungary or a country outside the EU, you may lodge a complaint with the Hungarian authority:

Contact details of the National Authority for Data Protection and Freedom of Information:

1055 Budapest, Falk Miksa u. 9-11.

Mailing address: 1363 Budapest, P.O. Box: 9.

Telephone: +36 (30) 683-5969, +36 (30) 549-6838, +36 (1) 391 1400

Fax: +36 (1) 391-1410

bv English language e-mail address: privacy(at)naih.hu

Hungarian language e-mail address: ugyfelszolgalat(at)naih.hu

Web: http://naih.hu

2. Right to appeal to court (right to bring an action)

The Data Subject – regardless of his/her right to complain – may appeal to court if, in his/her opinion, his/her rights under the GDPR have been violated during the processing of his/her personal data.

Proceedings against the data controller or data processor shall be initiated before the court of the EU Member State in which the data controller or data processor is established. Such proceedings may also be initiated before the court of the EU Member State in which the Data Subject has his/her habitual residence.

In Hungary, the trial falls within the competence of the court. The trial may also be initiated - at the choice of the Data Subject - before the court of the place of residence or residence of the Data Subject.

The contact details of the courts in Hungary can be found at the following link: http://birosag.hu/torvenyszekek.

The Data Subject may also initiate the lawsuit before the competent court of the Member State of habitual residence, if the Data Subject has his/her habitual residence in another Member State of the European Union.

The Data Controller reserves the right to amend the Notice at any time. The Data Controller shall notify the Data Subject of the amendment by publishing it on the website at least 8 days before the amendment comes into force.

Effective: from 16 February 2024

Budapest, 07 February 2024

Managing Director

Norbert Balázs dr.

Data Protection Officer

Data Protection Regulation

CFR Kft.

Annex No. 1

Valid from: 01.01.2025

until revocation

In preparing this data protection regulation, we have taken into account the following legal standards:

● Regulation (EU) 2016/679 of the European Parliament and of the Council (April 27, 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 Regulation 95/46/EC (General Data Protection Regulation, hereinafter referred to as: GDPR)

● Guidelines No. 3/2019 on the processing of personal data by video devices

● Act CXII of 2011 on the right to informational self-determination and freedom of information Act (Infotv.)

● Act V of 2013 on the Civil Code (Ptk.)

● Act C of 2000 on Accounting (Sztv.)

● Act CL of 2017 on the Taxation System

● Act CXXVII of 2007 on Value Added Tax (hereinafter: "VAT")

● Act CVIII of 2001 on certain issues of electronic commerce services and services related to the information society

● Act XLVIII of 2008 on the basic conditions and certain limitations of economic advertising activities

● Act CLV of 1997 on Consumer Protection (Fgytv.),

● Act CXXXIII of 2005 Act on the rules of personal and property protection and private investigation activities

Budapest, 01.01.2025

Managing Director

Privacy Policy

CFR Ltd.

Annex No. 2

Valid from: 01.01.2025

until revocation

Name of the company performing payroll accounting for our employees:

Mind Business Ltd. (1162 Budapest, Andrássy út 76., 1st floor, door 1

Name of the business entity performing the Company's accounting tasks:

Mind Business Kft. (1162 Budapest, Andrássy út 76., 1st floor, door 1

Our Company partially uses the assistance of IT service provider(s) according to the following

according to:

Name, registered office, task description of data processor

CFR Kft., 1135. Bp. Szegedi út 27., website operation,

Hostware Kft., 1149. Bp. Róna u.120-122.,

Performance of customer management tasks in case of using the Hostware Front Office hotel system.

The fire and occupational safety representative for the building is:

Queen Road Kft.

2030 Érd, Gábor utca 15/A.

Annamária Nagy, Managing Director

Budapest, 01.01.2025

Managing Director

Data Protection Regulation

CFR Ltd.

Annex No. 3

Valid from: 03.01.2025

until revocation

From January 1, 2025, the data will be partially transferred electronically to the accounting company:

Mind Business Ltd. (1162 Budapest, Andrássy út 76., 1st floor, door 1)

through the Cashbook

(Cashbook SBA Group Zrt., 1108 Budapest, Bányató utca 13.,

info@cashbook.hu,

+36 1/998-8506) system.

Budapest, 03.01.2025

Managing Director

Privacy Policy
CFR Ltd.
Annex No. 4
Valid from: 16.02.2024.
Until revocation

Location of the cameras installed in the premises of CFR Economic Consulting Ltd. at 1135 Budapest, Szegedi út 27. and description of the area monitored by them.

Floor	Camera Number	Position of camera	Monitored area
1.	Camera **01**	Entering the corridor, on the right side, in the middle	Corridor area, staircase entrance/exit and room doors from the corridor direction
	Camera **02**	Entering the corridor, on the right side, in the middle	Corridor area, room doors from the corridor direction
	Camera **03**	Entering the corridor, on the left side, in the middle	Corridor area, staircase entrance/exit and room doors from the corridor direction
	Camera **04**	Entering the corridor, on the left side, towards the middle	Corridor area and room doors from the corridor direction
	Kamera **05**	Above the front door on the left side	Kitchen area
	Camera **06**	Above the front door	Water block foyer

2.	Camera **01**	Entering the corridor, on the right side, in the middle	Corridor area, staircase entrance/exit and room doors from the corridor direction
	Camera **02**	Entering the corridor, on the right side, in the middle	Corridor area, room doors from the corridor direction
	Camera **03**	Entering the corridor, on the left side, in the middle	Corridor area, staircase entrance/exit and room doors from the corridor direction
	Camera **04**	Entering the corridor, on the left side, towards the middle	Corridor area and room doors from the corridor direction
	Camera **05**	Above the front door on the right side	Kitchen area
	Camera **06**	Above the front door	Water block foyer

3.	Camera **01**	Entering the corridor, on the right side, in the middle	Corridor area, staircase entrance/exit and room doors from the corridor direction
	Camera **02**	Entering the corridor, on the right side, in the middle	Corridor area, room doors from the corridor direction
	Camera **03**	Entering the corridor, on the left side, in the middle	Corridor area, staircase entrance/exit and room doors from the corridor direction
	Camera **04**	Entering the corridor, on the left side, towards the middle	Corridor area and room doors from the corridor
	Camera **05**	Above the front door on the left side	Kitchen area
	Camera **06**	Above the front door	Water block foyer

4.	Camera **01**	Entering the corridor, on the right side, in the middle	Corridor area, staircase entrance/exit and room doors from the corridor direction
	Camera **02**	Entering the corridor, on the right side, in the middle	Corridor area, room doors from the corridor direction
	Camera **03**	Entering the corridor, on the left side, in the middle	Corridor area, staircase entrance/exit and room doors from the corridor direction
	Camera **04**	Entering the corridor, on the left side, towards the middle	Corridor area and room doors from the corridor
	Camera **05**	Above the front door	Kitchen area
	Camera **06**	Above the front door	Water block foyer

5.	Camera 5th floor	The stairs to the 5th floor are located on the right side of the turn.	Staircase turn, entrance to apartment 501

Elevator	Camera **13**	Upper right corner when entering the elevator	Elevator area

12.02.2024., Budapest

Managing Director