DATA PROTECTION POLICY

General provisions

I. Details of the service provider as data controller

Róna Management Limited Liability Company

registered office: 1191 Budapest, Kossuth tér 23.

tax number: 32116678-2-43

company registration number: 01-09-407468

represented by: Katalin Ida Rónaszéki

telephone number: +36 70 398 8848

e-mail: reception@hotelallora.hu

(hereinafter: the "Data Controller")

The operator of Hotel Allora (hereinafter referred to as the Hotel), as data controller, hereby informs its customers, guests, and website visitors (hereinafter collectively referred to as: data subjects, users, or guests) that it respects the personal rights of all guests and conducts its data processing activities in accordance with the following privacy policy (hereinafter: Policy).

The data controller reserves the right to adapt the Policy to any changes in the law and to the internal regulatory environment and to amend it accordingly. The current version of the Policy is available on the website www.hotelallora.hu and can also be viewed in paper form at the Hotel reception.

This Policy regulates the data processing activities related to the services provided by Hotel Allora, operating at 1191 Budapest, Kossuth tér 23, and carried out through the Hotel's website.

I. PURPOSE OF THE REGULATIONS

1. The primary purpose of this Policy is to define and enforce the basic principles and provisions relating to the processing of data of natural persons – guests – who come into contact with the Hotel. The Policy ensures that the privacy of data subjects is protected in accordance with the relevant legal requirements.

2. Based on the provisions of Section I.1, the purpose of the Policy is to ensure that the Hotel's data processing practices comply in all respects with the applicable laws, in particular, but not exclusively, the following:

• Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR), which regulates the protection of personal data of natural persons and the free movement of such data, and repealed Directive 95/46/EC,

• Act CXII of 2011 on the right to self-determination in information and freedom of information,

• Act CVIII of 2001 on electronic commerce services and information society services,

• Act XLVII of 2008 on the prohibition of unfair commercial practices against consumers,

• Act XLVIII of 2008 on the basic conditions and certain restrictions of economic advertising activities.

The Data Controller attaches particular importance to ensuring the protection of personal data provided by data subjects on the website, other online platforms, or by other means. To this end, the Hotel fully complies with the above legislation, respects the right of data subjects to self-determination in relation to information, and contributes to the creation of conditions for safe internet use.

II. SCOPE OF THE REGULATIONS

1. Temporal scope: These Regulations shall be effective from December 10, 2025 until further notice or revocation.

2. Personal scope

The scope of the Regulations extends to:

1. the Data Controller,

2. the Hotel's employees and partners,

3. any person whose data is affected by data processing covered by these Regulations,

4. and those whose rights or legitimate interests are affected by data processing.

3. Scope of data subjects

Based on the provisions of points 2.iii. and 2.iv., data subjects include, in particular, natural persons who:

1. have used or requested the services of the Data Controller with the data provided on the Hotel's website,

2. have sent data to the email address reception@hotelallora.hu or through another forum for the purpose of establishing a customer relationship,

3. have sent data to the email address reception@hotelallora.hu or through another forum for other purposes, such as job seekers,

4. personally use the services provided by the Hotel.

4. Employees and partners

The Data Controller also processes the data of persons who are in an employee or partner relationship with it in separate data files.

5. Scope

This Policy applies to all data processing involving personal data carried out in all organizational units.

III. DEFINITIONS

Data subject / User / Guest: any natural person who can be identified directly or indirectly on the basis of their personal data. For example: a user booking a room through the website or a guest using the services of the Hotel.

Personal data: any information that can be linked to the data subject, in particular name, identification number, or physical, physiological, mental, economic, cultural, or social characteristics, as well as conclusions that can be drawn from these.

Hotel: Hotel Allora, operating at 1191 Budapest, Kossuth tér 23, operated by the Data Controller.

Consent: a voluntary and unambiguous statement by the data subject, based on adequate information, by which he or she agrees to the full or partial processing of his or her personal data.

Data controller: the natural or legal person or organization without legal personality who, alone or jointly with others, determines the purposes of data processing, decides on the methods and means of data processing, and carries out or has them carried out by a data processor.

Data processing: any operation or set of operations performed on data, regardless of the method used. This includes, in particular: collection, recording, organization, storage, modification, use, retrieval, disclosure, dissemination, alignment, blocking, erasure, destruction, as well as the creation of photographs, audio or video recordings and the recording of physical characteristics suitable for identification.

Data transfer: making personal data available to a specific third party.

Data processing: performing technical tasks related to data management, regardless of the method, tool, or location used, as long as it is done on the data.

Data erasure: rendering data unrecognizable in such a way that it can no longer be restored.

Data blocking: marking data with an identifier that permanently or temporarily restricts its further processing.

Data destruction: the complete physical destruction of the data carrier, which permanently removes the data.

Data file: the totality of data managed in a register.

Third party: any natural or legal person or organization without legal personality other than the data subject, the data controller, or the data processor.

Data breach: unlawful processing or processing of personal data, including unauthorized access, modification, transmission, disclosure, deletion, destruction, and accidental destruction or damage.

Partner: legal entities or business associations without legal personality that use the Data Controller's services on a contractual basis or facilitate the performance of those services. The Data Controller may, with the consent of the data subject, transfer personal data to them or use them for data storage, processing, IT and other secure data management tasks.

Data processors: organizations belonging to the Partners that perform data processing activities on behalf of the Data Controller. They are specifically named later in the Policy.

In addition to those named later in the Policy, data processors include, in particular:

IT service provider:

www.cts.hu

Address: 4029 Debrecen, Maróthy u. 3.

Phone: +36 52 521 420

Mobile: +36 20 260 3186

tarpai.boglarka@cts.hu

Employee: a natural person who is in a contractual, employment or other legal relationship with the Data Controller and who participates in the provision and performance of the Data Controller's services. In the course of their duties, they may come into contact with the handling or processing of personal data. The Data Controller assumes full responsibility for the activities of its Employees towards data subjects and third parties.

Website: the www.hotelallora.hu portal and all its subpages operated by the Data Controller.

Facebook page: https://www.facebook.com/hotelallora

instagram: www.instagram.com/hotel_allora

IV. DATA PROCESSING PRINCIPLES

1. The provisions of the Policy and the practices of the Data Controller shall not conflict with the basic principles of data processing.

2. From the date of publication of the Policy, the following data processing principles shall be introduced, which are binding and serve as guidelines even in cases not specifically regulated by the Policy:

Principle of purpose limitation: Personal data may only be processed for a specific purpose, for the exercise of a right or for the fulfillment of an obligation. All stages of data processing must be consistent with the purpose set out and must be fair and lawful.

Principle of proportionality and necessity: Only personal data that is essential and suitable for achieving the purpose may be processed. The duration and extent of data processing shall not exceed the limits necessary to achieve the purpose.

Principle of identifiability: Personal data retains its quality as long as the connection with the data subject can be re-established, i.e. the Data Controller has the necessary technical conditions.

Principle of accuracy and timeliness: During data processing, the accuracy, completeness and, where necessary, timeliness of the data must be ensured. The identification of the data subject may only be retained for as long as is necessary to achieve the purpose.

Principle of security: The Data Controller shall protect personal data stored in automated data files from accidental or unlawful destruction, loss, unauthorized access, modification, or dissemination by means of appropriate technical and organizational measures.

Principle of voluntariness and consent: The provision of data is voluntary on the part of the data subject, and the Data Controller processes personal data with the consent of the data subject. The user's behavior also constitutes consent when, by using the website, the data subject accepts the rules applicable to him or her, or when, after receiving prior information, he or she enters the hotel area monitored by the camera system.

Principle of data transfer: The Data Controller shall only transfer personal data to third parties in exceptional cases, and shall only link its database with that of another data controller if the data subject expressly consents to this, or if this is permitted by law and all data processing conditions are met.

Principle of partner data transfer: For the purposes of the Data Controller's services and data processing, the Guest expressly agrees that the Data Controller may transfer their personal data to its previously named partners if their cooperation facilitates the performance of the service.

Prohibition of international data transfer: The Data Controller shall not transfer personal data to a data controller or data processor operating in a third country.

IV/A LEGAL BASIS FOR DATA PROCESSING

1. The legal basis for data processing is the voluntary consent of the data subject, which is given to the Data Controller on the basis of prior, adequate information.

2. If the processing of personal data is required by law, data processing is mandatory. In such cases, the Data Controller shall inform the data subject, including Employees and Partners.

3. If the personal data has been recorded with the consent of the data subject, the Data Controller may process the data, unless otherwise provided by law, in order to fulfill its legal obligations or to enforce its own or a third party's legitimate interests. This is only possible if the enforcement of the legitimate interest is proportionate to the restriction of the data subject's right to the protection of personal data. No further consent is required for such data processing, and it may be continued even after the data subject has withdrawn their consent. The Data Controller shall in all cases inform the data subject if their personal data is processed on this legal basis.

IV/B DURATION OF DATA PROCESSING

1. The duration of data processing shall be until the data subject requests the deletion of their personal data or revokes their consent to data processing. If no such provision is made, and unless otherwise provided by law, the duration of data processing shall be three years after the expiry of the enforceability of the rights and obligations arising from the legal relationship in question.

2. The Policy may stipulate a different time limit from that specified in point 1 for certain data processing operations.

3. You may request the modification or deletion of your personal data, the withdrawal of your consent, or information about data processing by sending a notification to reception@hotelallora.hu.

V. STATEMENTS BY THE DATA CONTROLLER

1. The Data Controller declares that:

1. During data processing, it acts in accordance with the provisions of Act CXII of 2011 (on the right to self-determination and freedom of information) and Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR).
2. Personal data shall only be accessible to those Employees whose job description includes the performance of the given data processing task.
3. It shall ensure that the Regulations in force at any given time are continuously accessible to the data subjects, thereby enforcing the principle of transparency.
4. The personal data of visitors to the website shall be treated confidentially in accordance with the law, their security shall be ensured, technical and organizational measures shall be applied, and procedural rules shall be established to ensure full compliance with data protection principles.

5. The personal data of guests staying at the hotel is treated confidentially, in accordance with applicable laws, and its protection is ensured through the application of appropriate technical, organizational, and procedural measures for data protection.
6. During data storage, processing, and transfer, all necessary IT and security measures are taken to ensure data preservation.
7. It shall do everything that can be expected of it to ensure that the personal data processed is protected against unauthorized access, modification, disclosure, deletion, damage or destruction, and shall guarantee the necessary technical conditions.
8. It does not verify the personal data provided by the data subjects and does not assume responsibility for their accuracy.
9. It only transfers personal data to third parties in exceptional cases and only links its database with that of another data controller if the data subject expressly consents to this or if it is permitted by law and all data processing conditions are met.
10. It operates exclusively in Hungary and does not belong to a multinational hotel chain, therefore the introduction and operation of mandatory organizational regulations is not necessary.
11. Personal data shall not be transferred to a data controller or data processor operating in a third country.
12. It shall keep a record of data protection incidents, which shall include the scope of the personal data concerned, the number and scope of persons affected by the incident, the date, circumstances and effects of the incident, the measures taken to remedy the situation, and other data required by law.

2. The Data Controller shall not be liable for the lawfulness of data processing by its contractual partners.

3. The Data Controller shall protect personal data stored in automated data files from accidental or unlawful destruction, loss, unauthorized access, modification, or dissemination by means of appropriate security measures.

VI. ACTIVITIES AND DATA AFFECTED BY DATA PROCESSING

VI.1 Use of hotel services

1. When using hotel services, the processing of personal data is based on voluntary consent. The purpose of data processing is to provide services and maintain contact. The Data Controller shall store the personal data specified in this section, with the exceptions set out in the sub-sections, in accordance with current tax and accounting regulations, and shall delete them upon expiry of the data processing period.

2. When using certain services, it is possible to provide additional data to help us better understand the Guest's needs. However, providing this data is not a prerequisite for using the hotel's services.

3. The data subject may at any time request the deletion or blocking of the recorded and stored data, or request detailed information about the data processing. This can be done by

sending a request to reception@hotelallora.hu, unless other contact details are provided for the data processing activity in question.

VI.2 Room reservation

1. When booking a room, the Data Controller may request the following information from the Guest on its website:

• First name*

• Last name*

• Email*

• Phone number*

• Date of arrival*

• Date of departure*

• Number of adults*

• Number of children, infants*

• Room type*

• Address*

• If you are booking a room with non-refundable cancellation terms, your credit card details*

• Comments

2. The activities and processes involved in data processing are as follows:

a. The data subject checks the availability for the desired period on the Hotel's website. If there is availability, they initiate the room reservation electronically by clicking on the "Reserve" button and providing the necessary personal data (name, email address, telephone number, address), thereby accepting this privacy policy and the terms and conditions available on the website.

b. The data provided by the data subject will be sent to the Hotel by email.

c. The Data Controller's receptionist, finance or sales staff will manually enter the data provided by the data subject into the electronic booking system and link it to the appropriate room, thereby creating the booking.

d. The data subject receives written confirmation of the reservation by email in the form of a system message. The sales staff records the data provided during the reservation in the Hostware (HostWare Kft.; company registration number: 01-09-263594; registered office: 1149 Budapest, Róna utca 120.) and D-edge (https://d-edge.com) software used by the Data Controller.

e. In the case of non-refundable credit card reservations, the relevant credit card number and expiration date will be forwarded to the Data Controller.

3. Room reservations at the Data Controller's Hotel are also available on the following room reservation websites:

- www.booking.com
- www.szallas.hu
- www.hrs.com
- www.expedia.com
- www.szallas.hu
- www.veturis.com
- www.lastminute.com
- www. g2-travel.com
- www.tripmakery.com
- aicgroup.biz
- www.mgbedbank.com
- www.emergingtravel.com
- https://www.makemytrip.global
- www.hoteltonight.com
- www.hotelbeds.com

The purpose of our presence on room booking websites and the related data processing is to provide Guests with the widest possible range of room booking options. Detailed information on the data processing practices of individual intermediary websites is provided in the privacy policies and regulations published on the websites of the respective service providers, which can be accessed at the following links:

- www.booking.com
- www.szallas.hu
- www.hrs.com
- www.expedia.com
- www.szallas.hu
- www.veturis.com
- www.lastminute.com
- www. g2-travel.com
- www.tripmakery.com
- aicgroup.biz
- www.mgbedbank.com
- www.emergingtravel.com
- https://www.makemytrip.global

- www.hoteltonight.com
- www.hotelbeds.com

4. The Data Controller shall retain personal data related to canceled reservations for a maximum of 6 months, after which it shall be destroyed, unless applicable tax or accounting regulations stipulate a longer retention period.

VI.3 Registration and registration form

1. Upon arrival at the Hotel, the data subject shall fill out a hotel registration form before occupying the reserved room. By doing so, the data subject consents to the Data Controller processing the data provided therein for the purpose of fulfilling and verifying its obligations under the relevant legislation, in particular the regulations on immigration and tourist tax, and for the purpose of identifying the Guest, for as long as the competent authority can verify the fulfillment of these obligations.

• Date of arrival*

• Date of departure*

• Room number*

• Surname*

• First name*

• Date of birth*

• Place of birth*

• Nationality*

• Passport number*

• Address*

• Email address

• Status under 18 years of age

• Legal basis for exemption from tourist tax

2. The provision of mandatory data by the Guest is a prerequisite for the use of hotel services.

3. By signing the registration form, the Guest consents to the Data Controller processing and archiving the personal data provided therein within the specified time limit for the purposes of concluding, performing and verifying the contract, as well as for the enforcement of any claims.

4. The email address provided on the registration form allows the Guest to subscribe to the Data Controller's newsletter. The rules governing the newsletter are set out in Section VI.6.

VI.4 Sending newsletters

1. The data subject may subscribe to the newsletter on the website or by email by providing the specified personal data.

2. The detailed rules for data processing related to sending the newsletter are contained in a separate data processing notice, which is available on the website www.hotelallora.hu.

VI.5 Bank card details

1. During the booking process, the Data Subject may provide credit card details on the Data Controller's website.

2. Scope of data processed:

Credit card number*

Expiration date*

CVV code*

3. The Data Controller shall process the bank card details provided by the data subject on the secure interface in accordance with this data processing policy and shall store them separately in the booking system. Special authorization is required to view the data, thus ensuring the protection of bank card details.

4. The Data Controller shall use the credit card details only to the extent and for the period necessary to exercise its rights or fulfill its obligations. In the case of a non-refundable reservation, the credit card will be charged at the time of booking, in other cases at the time of the Guest's departure. Beyond this, credit card data is processed by banking partners, whose data processing practices can be found on the official website of the bank concerned.

5. The Data Controller's banking partner, which operates the credit card terminal, is as follows:

Teya Services Ltd.
Milton Gate, 60 Chiswell Street, London, United Kingdom, EC1Y 4AG

6. Guests may obtain further information regarding the bank card data processed by certain subsystems of the Data Controller by sending a request to reception@hotelallora.hu.

VI.6 Camera system

1. A camera system operates on the premises of the Hotel operated by the Data Controller for the purpose of protecting the personal safety and property of Guests. Signs inform those concerned of the presence of cameras. The Data Controller ensures the lawful operation of

the system in accordance with the provisions set out in these Rules and in the separate Camera Rules, which are available to those concerned.

2. Scope of data processed: image and sound recordings made by the camera system.

3. Special rules for camera surveillance:

1. The operation of the camera system is governed by a separate regulation, the current version of which is available at the Hotel reception.
2. The system records both video and audio.
3. The purpose of data processing: protection of persons and property.
4. The storage location of the recordings: the Hotel (1191 Budapest, Kossuth Square 23.), operated by the Data Controller.
5. The legal basis of data processing is the voluntary consent of the data subject, given on the basis of the posted information signs. Consent may also be expressed by implied conduct, for example by entering or remaining in an area monitored by cameras.
6. The Data Controller is obliged to protect the personal data of the data subjects – especially their secrets and circumstances of private life – from unauthorized access.
7. Electronic surveillance systems may not be used in places where they would violate human dignity (e.g. changing rooms, showers, washrooms, toilets, rest areas). Surveillance is always purpose-bound and proportionate; the Data Controller does not carry out unlimited or direct monitoring.
8. Storage period of recordings: in the absence of use, a maximum of 3 working days, after which they must be deleted or destroyed. Use is defined as when the recording or other personal data is applied as evidence in court or authority proceedings.
9. The data subject whose right or legitimate interest is affected by the recording may request – within 3 working days from the recording – with proof of their right or legitimate interest, that the data not be deleted or destroyed.
10. In the event of a request from a court or authority, the recorded footage and other personal data must be forwarded without delay. If the request does not arrive within 30 days, the recording must be deleted or destroyed, unless the deadline specified in the Regulation has not yet expired.

VI.7 Social media

The Hotel operated by the Data Controller is present on the social media platforms Facebook, Instagram, and TikTok.

The purpose of appearing on social media platforms and the related data processing is to share, publish, and market the content found on the website. Through social media, Guests can be informed about the latest promotions and offers.

By clicking the “like” button on the Data Controller’s social media pages, the data subject consents to the Data Controller’s news and offers appearing on their own news feed.

On the Data Controller's social media pages, photos and videos are published about the Hotel, events, and other content. In cases other than mass recordings, the written consent of the data subject is always required before publication.

Information about the data processing practices of social media platforms can be found in the privacy policies and regulations published on the respective provider's website.

VI.8 Website visitors data

1. VI.15.1 References and Links

1. The Data Controller's website may contain links that lead to sites not operated by the Data Controller, serving solely to inform visitors. The Data Controller has no influence over the content or security of websites operated by partner companies and therefore assumes no responsibility for them.
2. We recommend that you always review the data management policies and privacy statements of any websites you visit before providing personal data in any form.

2. VI.15.2 Analytics, cookies

1. In accordance with Section 155 (4) of Act C of 2003, the Data Controller informs users about the analytical tools it employs, namely cookies. Under the law, data may be stored on or accessed from an electronic communications device only with the prior consent of the data subject, following full and comprehensive information.

2. Usage of cookies

1. Cookies are small data files placed on the user's computer by the website visited. Their purpose is to make internet services more convenient and efficient. There are two main types:

- **Temporary cookies**: stored only for the duration of the session (for example, during online banking).
- **Permanent cookies**: remain on the user's device until they are manually deleted (for example, saving language settings).

According to the guidelines of the European Commission, cookies – with the exception of those strictly necessary – may only be placed with the user's consent.

1. For cookies that do not require consent, a brief notice appears upon the first visit to the website, which includes a link to the full policy.
2. For cookies that require consent, the notice appears upon the first visit to the website or when using the relevant function. In such cases, a short summary is sufficient, provided it includes a link to the detailed information

Information about the usage of cookies

1. The Data Controller's website uses cookies in accordance with international practice. These allow the browser to be recognized, user settings (e.g., language) to be saved, and the operation of online services – such as a shopping cart – to function. Cookies make the use of the website more convenient, while for the operator they ensure monitoring of operation, prevention of misuse, and the appropriate quality of services.
2. During a visit, the website records the following data:
   IP address
   Type of browser
   Characteristics of the operating system (e.g., selected language)
   Time of visit
   Subpages, functions, and services visited
3. The use of cookies is not mandatory. The user can set their browser to reject all cookies or to notify them when the system sends a new cookie. Although most browsers accept cookies by default, this can be changed. If cookies are disabled, certain functions may not operate properly.
4. The cookies used on the website are not suitable on their own for identifying the user personally.

Types of cookies used by the Data Controller:

1. Strictly necessary cookies – essential for the operation of the website, they do not collect data for marketing purposes.
2. Functional cookies – remember the user's settings (e.g., color, font size, layout).
3. Targeting cookies – tailor advertisements to the user's interests.
4. Third-party cookies – for example, cookies provided by social media platforms that enable sharing or liking, and may also be used for advertising purposes.

Analytical tools:
The Data Controller uses the Google Analytics service to collect anonymous data (e.g., visitor numbers, browsing habits). Google Inc. may also use this data to display targeted advertisements. Detailed information is available on the Google Analytics support page.

Browser settings:
The user may delete or disable cookies at any time. Information about the settings of the most popular browsers can be found at the following links.

- Google Chrome
- Firefox
- Microsoft Edge

- Safari
  (as well as separate links available for earlier versions of Internet Explorer).

VII. STORAGE OF PERSONAL DATA AND INFORMATION SECURITY

1. Personal data may only be processed in accordance with the activities defined in Chapter VI and in line with the purpose of data processing.
2. The Data Controller ensures the protection of data by taking the necessary technical and organizational measures regarding the data files stored on IT systems.
3. The Data Controller guarantees full compliance with the data security requirements prescribed by applicable legislation.
4. To ensure data security, the Data Controller establishes and applies the necessary technical, organizational, and procedural rules that comply with relevant laws as well as data and confidentiality protection requirements.
5. The Data Controller protects data against unauthorized access, alteration, transmission, disclosure, deletion, destruction, and accidental damage or loss. It also ensures that changes in technology do not result in data becoming inaccessible.
6. The enforcement of data security rules may also be ensured by the Data Controller through separate regulations, instructions, and procedures.
7. Employees of the Data Controller are required to act in accordance with the provisions set out in this Policy, as well as in other data protection regulations, job descriptions, and instructions, thereby guaranteeing a high level of data security.
8. The Data Controller ensures that its employees receive appropriate training to meet data security requirements.
9. When defining and applying data security measures, the Data Controller takes into account the current state of technological development and chooses the solution that provides the highest level of protection for personal data, unless this would cause disproportionate difficulty.
10. Within the scope of IT protection, the Data Controller particularly ensures:

    Protection against unauthorized access, including software, hardware, and physical security (access and network protection).

    Restorability of data files, regular backups, and the secure, separate handling of copies.

    Protection against viruses.

Physical protection of data files and the devices carrying them, especially against fire, water, lightning, and other natural disasters, as well as restoration after such events.

11. The Data Controller ensures the IT environment in such a way that:
    - Personal data provided by the data subject is linked only in the manner defined in this Policy.
    - Access to personal data is granted only to employees who need it to perform their job duties.
    - All data changes are recorded with a timestamp.
    - Incorrect data is deleted within 24 hours at the request of the data subject.
    - Backups of the data are created.
12. The Data Controller guarantees that the handling of data – including storage, correction, and deletion – is carried out at the required level of protection even in cases where the data subject requests information or raises an objection.
13. Data transfer may only take place with the consent of the data subject, without prejudice to their interests, confidentially, and with appropriate IT protection, in compliance with the purpose, legal basis, and principles of data processing. The Data Controller does not transfer personal data to third parties without consent, except where required by law.
14. Data that cannot be directly or indirectly linked to the data subject and is unidentifiable – i.e., anonymous data – is not considered personal data.

SUMMARY INFORMATION ON THE RIGHTS OF THE DATA SUBJECT

For clarity and transparency, this subsection provides a brief summary of the rights of the data subject, while detailed information on the exercise of these rights is contained in the following chapter.

Right to prior information

The data subject has the right to be informed of the facts and details related to data processing before it begins.
(Based on Articles 13–14 of the General Data Protection Regulation of the European Union)
The detailed rules are set out in the next subsection.

Right of access

The data subject has the right to receive confirmation from the Data Controller as to whether their personal data is being processed. If such processing is taking place, the data subject is entitled to access the personal data being processed, as well as the related information specified in the Regulation.
(Based on Article 15 of the General Data Protection Regulation of the European Union)
The detailed rules are set out in the next subsection.

Right to Rectification

The data subject has the right to request that the Data Controller correct inaccurate personal data concerning them without undue delay. Taking into account the purpose of the processing, the data subject also has the right to request the completion of incomplete personal data – for example, by submitting a supplementary statement.
(Based on Article 16 of the General Data Protection Regulation of the European Union)

Right to Erasure ("Right to be Forgotten")

1. The data subject has the right to request that the Data Controller erase personal data concerning them without undue delay. The Data Controller is obliged to carry out such erasure immediately if one of the conditions specified in the Regulation applies. (Based on Article 17 of the General Data Protection Regulation of the European Union)
   The detailed rules are set out in the next subsection.

Right to Restriction of Processing

The data subject has the right to request that the Data Controller restrict the processing of their personal data if the conditions specified in the Regulation are met.
(Based on Article 18 of the General Data Protection Regulation of the European Union)
The detailed rules are set out in the next subsection.

Obligation to Notify Regarding Rectification, Erasure, or Restriction of Processing

The Data Controller shall inform all recipients to whom the personal data has been disclosed of any rectification, erasure, or restriction of processing, unless this proves impossible or requires disproportionate effort. At the request of the data subject, the Data Controller shall provide information about those recipients.
(Based on Article 19 of the General Data Protection Regulation of the European Union)

Right to Data Portability

Under the conditions specified in the Regulation, the data subject has the right to receive the personal data they have provided to the Data Controller in a structured, commonly used, and machine-readable format. They also have the right to transmit this data to another Data Controller without hindrance, regardless of which Data Controller originally received the data.
(Based on Article 20 of the General Data Protection Regulation of the European Union)
The detailed rules are set out in the next subsection.

Right to Object

The data subject has the right, on grounds relating to their particular situation, to object at any time to the processing of their personal data if the processing is carried out under Article 6(1)(e) of the Regulation for the performance of a task carried out in the public interest or in

the exercise of official authority vested in the Data Controller, or under Article 6(1)(f) for the purposes of the legitimate interests pursued by the Data Controller or by a third party.
(Based on Article 21 of the General Data Protection Regulation of the European Union)
The detailed rules are set out in the next subsection.

Automated Individual Decision-Making, Including Profiling

The data subject has the right not to be subject to a decision based solely on automated processing – including profiling – which produces legal effects concerning them or similarly significantly affects them.
(Based on Article 22 of the General Data Protection Regulation of the European Union)
The detailed rules are set out in the next subsection.

Restrictions

Union or Member State law applicable to the Data Controller or the data processor may, by legislative measures, restrict the application of the rights and obligations set out in Articles 12–22 and 34, as well as those defined in Articles 12–22.
(Based on Article 23 of the General Data Protection Regulation of the European Union)
The detailed rules are set out in the next subsection.

Information to the Data Subject about a Data Protection Incident

If a data protection incident is likely to result in a high risk to the rights and freedoms of natural persons, the Data Controller is obliged to inform the data subject of the incident without undue delay.
(Based on Article 34 of the General Data Protection Regulation of the European Union)
The detailed rules are set out in the next subsection.

Right to Lodge a Complaint with a Supervisory Authority (Right to Administrative Remedy)

The data subject has the right to lodge a complaint with a supervisory authority – in particular in the Member State of their habitual residence, place of work, or the place of the alleged infringement – if they consider that the processing of their personal data infringes the provisions of the Regulation.
(Based on Article 77 of the General Data Protection Regulation of the European Union)
The detailed rules are set out in the next subsection.

Right to an Effective Judicial Remedy Against a Supervisory Authority

Every natural and legal person has the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them. This right also applies if the supervisory authority does not handle a lodged complaint or fails to inform the data subject within three months about the progress or outcome of the complaint procedure.
(Based on Article 78 of the General Data Protection Regulation of the European Union)
The detailed rules are set out in the next subsection.

Right to an Effective Judicial Remedy Against the Data Controller or Processor

Every data subject has the right to an effective judicial remedy if they consider that the processing of their personal data does not comply with the provisions of the Regulation and thereby infringes the rights guaranteed to them under the Regulation.
(Based on Article 79 of the General Data Protection Regulation of the European Union)

DETAILED INFORMATION ON THE RIGHTS OF THE DATA SUBJECT

Right to Prior Information

The data subject's right to information before the commencement of data processing
The data subject is entitled to receive detailed information about the facts and circumstances of data processing before it begins.

A) Information when personal data is collected directly from the data subject

1. When data is obtained directly from the data subject, the Data Controller is obliged to provide the following information at the time of collection:

- The identity and contact details of the Data Controller and, if applicable, its representative.
- The contact details of the data protection officer (if one has been appointed).
- The purpose and legal basis of the data processing.
- In the case of processing based on legitimate interests, the legitimate interests pursued by the Data Controller or a third party.
- The recipients or categories of recipients of the data (if any).
- If the data is to be transferred to a third country or international organization, the fact of such transfer, as well as the appropriate safeguards and how they can be accessed.

2. For fair and transparent data processing, the Data Controller is also obliged to provide additional information:

- The period of storage of the data, or the criteria used to determine that period.
- The rights of the data subject (access, rectification, erasure, restriction, objection, data portability).
- In the case of processing based on consent, the right to withdraw consent at any time.
- The right to lodge a complaint with a supervisory authority.

- Clarification of whether the provision of data is a statutory or contractual requirement, or a prerequisite for entering into a contract, and the possible consequences of failing to provide the data.
- The existence of automated decision-making (including profiling), the logic involved, and the expected consequences of such processing.

3. If the data is to be used for a purpose other than that for which it was collected, the data subject must be informed in advance about this and the related information.
4. The obligation to provide information does not apply if the data subject already has the information.

(Based on Article 13 of the General Data Protection Regulation of the European Union)

B) Information When Personal Data Is Not Obtained Directly from the Data Subject

1. In this case, the Data Controller must provide the data subject with:

- The identity and contact details of the Data Controller and, if applicable, its representative.
- The contact details of the data protection officer (if appointed).
- The purpose and legal basis of the data processing.
- The categories of personal data concerned.
- The recipients or categories of recipients of the data.
- If the data is to be transferred to a third country or international organization, the fact of such transfer, as well as the appropriate safeguards and how they can be accessed.

2. For fair and transparent data processing, the Data Controller must also provide additional information:

- The period of storage of the data, or the criteria used to determine that period.
- In the case of processing based on legitimate interests, the legitimate interests pursued by the Data Controller or a third party.
- The rights of the data subject (access, rectification, erasure, restriction, objection, data portability).
- In the case of processing based on consent, the right to withdraw consent at any time.
- The right to lodge a complaint with a supervisory authority.
- The source of the data, and, where applicable, whether it originates from publicly accessible sources.

- The existence of automated decision-making (including profiling), the logic involved, and the expected consequences of such processing.

3. The Data Controller must provide this information:

- Within a reasonable period after obtaining the data, but no later than one month.
- If the data is used for communication purposes, at the time of the first contact.
- If the data is disclosed to another recipient, at the latest at the time of the first disclosure.

4. If the data is to be used for a purpose other than that for which it was obtained, the data subject must be informed in advance about this and the related information.
5. The obligation to provide information does not apply if:
    1. The data subject already has the information.
    2. Providing the information proves impossible or would involve disproportionate effort (e.g., in cases of archiving, research, or statistical purposes).
    3. The obtaining or disclosure of the data is required by Union or Member State law, which provides appropriate safeguards.
    4. The data is confidential due to professional secrecy obligations.

(Based on Article 14 of the General Data Protection Regulation of the European Union)

Right of Access

1. The data subject has the right to obtain confirmation from the Data Controller as to whether or not personal data concerning them is being processed. If such processing is taking place, the data subject is entitled to access the personal data and the following information:
2. The purposes of the processing.
3. The categories of personal data concerned.
4. The recipients or categories of recipients to whom the personal data has been or will be disclosed, in particular recipients in third countries or international organizations.
5. Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period.
6. The rights of the data subject: access, rectification, erasure, restriction of processing, and the right to object.
7. The right to lodge a complaint with a supervisory authority.
8. Where the personal data is not collected directly from the data subject, any available information about its source.

9. The existence of automated decision-making, including profiling, as well as meaningful information about the logic involved, and the significance and envisaged consequences of such processing for the data subject.
10. Where personal data is transferred to a third country or international organization, the data subject has the right to be informed of the appropriate safeguards relating to the transfer in accordance with Article 46 of the Regulation.
11. The Data Controller is obliged to provide the data subject with a copy of the personal data undergoing processing. For any further copies requested by the data subject, the Data Controller may charge a reasonable fee based on administrative costs. Where the request is made electronically, the information shall be provided in a commonly used electronic format, unless the data subject requests otherwise. The right to obtain a copy must not adversely affect the rights and freedoms of others.

(Based on Article 15 of the General Data Protection Regulation of the European Union)

Right to Erasure ("Right to be Forgotten")

1. The data subject has the right to request that the Data Controller erase personal data concerning them without undue delay. The Data Controller is obliged to carry out such erasure immediately if any of the following conditions apply:
   The personal data is no longer necessary for the purpose for which it was collected or processed.
   The data subject withdraws their consent (under Article 6(1)(a) or Article 9(2)(a) of the Regulation), and there is no other legal basis for the processing.
   The data subject objects to the processing (under Article 21(1) or (2)), and there are no overriding legitimate grounds for the continuation of the processing.
   The personal data has been unlawfully processed.
   The personal data must be erased to comply with a legal obligation under Union or Member State law applicable to the Data Controller.
   The personal data was collected in connection with the provision of information society services as referred to in Article 8(1) of the Regulation.
2. Where the Data Controller has made the personal data public and is obliged to erase it, the Data Controller shall, taking account of available technology and the cost of implementation, take reasonably practicable steps – including technical measures – to inform other Data Controllers processing the data that the data subject has requested the erasure of any links to, copies of, or replications of that personal data.

(Based on Article 17 of the General Data Protection Regulation of the European Union)

Right to Restriction of Processing

1. The data subject has the right to request that the Data Controller restrict the processing of their personal data if any of the following conditions apply:
    1. The accuracy of the personal data is contested by the data subject; in this case, the restriction applies for the period during which the Data Controller verifies the accuracy of the data.
    2. The processing is unlawful, but the data subject opposes the erasure of the data and requests the restriction of its use instead.
    3. The Data Controller no longer needs the personal data for the purposes of processing, but the data subject requires it for the establishment, exercise, or defense of legal claims.
    4. The data subject has objected to processing pursuant to Article 21(1) of the Regulation; in this case, the restriction applies until it is determined whether the legitimate grounds of the Data Controller override those of the data subject.
2. Where processing has been restricted under point 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent, or for the establishment, exercise, or defense 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.
3. The Data Controller must inform the data subject in advance if it intends to lift the restriction imposed under point 1.

(Based on Article 18 of the General Data Protection Regulation of the European Union)

Right to Data Portability

1. The data subject has the right to receive the personal data they have provided to the Data Controller in a structured, commonly used, and machine-readable format. They also have the right to transmit this data to another Data Controller without hindrance if:
    1. The processing is based on the data subject's consent (Article 6(1)(a) or Article 9(2)(a) of the Regulation), or on a contract (Article 6(1)(b)); and
    2. The processing is carried out by automated means.
2. The data subject also has the right, where technically feasible, to request the direct transfer of their personal data from one Data Controller to another.
3. The exercise of the right to data portability shall not adversely affect the right to erasure as set out in Article 17 of the Regulation. This right does not apply where the

processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.

4. The exercise of the right to data portability must not infringe the rights and freedoms of others.

(Based on Article 20 of the General Data Protection Regulation of the European Union)

Right to Object

1. The data subject has the right, at any time and on grounds relating to their particular situation, to object to the processing of their personal data where the processing is based on Article 6(1)(e) of the Regulation (performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller) or Article 6(1)(f) (legitimate interests pursued by the Data Controller or a third party), including profiling carried out for such purposes. In such cases, the Data Controller shall no longer process the personal data unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights, and freedoms of the data subject, or for the establishment, exercise, or defense of legal claims.
2. Where personal data is processed for direct marketing purposes, the data subject has the right to object at any time to such processing, including profiling to the extent that it is related to direct marketing.
3. If the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.
4. The data subject must be explicitly informed of the rights set out in points 1 and 2 at the latest at the time of the first communication with them. This information must be presented clearly, prominently, and separately from any other information.
5. In the context of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise their right to object by automated means using technical specifications.
6. Where personal data is processed for scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the Regulation, the data subject has the right, on grounds relating to their particular situation, to object to the processing of personal data concerning them, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

(Based on Article 21 of the General Data Protection Regulation of the European Union)

Automated Individual Decision-Making, Including Profiling

1. The data subject has the right not to be subject to a decision – including profiling – based solely on automated processing, which produces legal effects concerning them or similarly significantly affects them.

2. The right set out in point 1 does not apply if the decision:
    1. Is necessary for entering into, or the performance of, a contract between the data subject and the Data Controller.
    2. Is authorized by Union or Member State law which provides suitable measures to safeguard the data subject's rights, freedoms, and legitimate interests.
    3. Is based on the data subject's explicit consent.
3. In the cases referred to in points 2(a) and 2(c), the Data Controller must implement measures to safeguard the data subject's rights, freedoms, and legitimate interests. This includes at least the right to obtain human intervention, to express their point of view, and to contest the decision.
4. Decisions referred to in point 2 must not be based on special categories of personal data as defined in Article 9(1) of the Regulation, unless Article 9(2)(a) or (g) applies and appropriate measures have been taken to protect the rights, freedoms, and legitimate interests of the data subject.

(Based on Article 22 of the General Data Protection Regulation of the European Union)

Restrictions

1. Union or Member State law applicable to the Data Controller or the data processor may, by legislative measures, restrict the application of the rights and obligations set out in Articles 12–22 and 34 of the Regulation, as well as those provided for in Article 5 in line with them. Such restrictions may only be applied if they respect the essence of fundamental rights and freedoms and constitute a necessary and proportionate measure in a democratic society for the protection of the following objectives:
    1. National security.
    2. Defense.
    3. Public security.
    4. The prevention, investigation, detection, or prosecution of criminal offenses or the execution of criminal penalties, including the protection against and prevention of threats to public security.
    5. Other important objectives of general public interest of the Union or of a Member State, in particular economic or financial interests (e.g., monetary, budgetary, taxation matters), public health, or social security.
    6. The protection of judicial independence and judicial proceedings.

7. The prevention, investigation, detection, and prosecution of breaches of ethics for regulated professions.
8. Monitoring, inspection, or regulatory functions connected to the exercise of official authority in the cases referred to in points (a)–(e) and (g).
9. The protection of the rights and freedoms of the data subject or of others.
10. The enforcement of civil law claims.

2. Legislative measures referred to in point 1 shall, where necessary, contain specific provisions at least regarding:

1. The purposes of the processing or categories of processing.
2. The categories of personal data concerned.
3. The scope of the restrictions introduced.
4. The safeguards to prevent abuse or unauthorized access or transmission.
5. The specification of the Data Controller or categories of Data Controllers.
6. The storage periods and the applicable safeguards, taking into account the nature, scope, and purposes of the processing.
7. The risks to the rights and freedoms of data subjects.
8. The right of data subjects to be informed about the restriction, unless this would jeopardize the purpose of the restriction.

(Based on Article 23 of the General Data Protection Regulation of the European Union)

Information to the Data Subject about a Data Protection Incident

1. If a data protection incident is likely to result in a high risk to the rights and freedoms of natural persons, the Data Controller is obliged to notify the data subject of the incident without undue delay.
2. The information provided to the data subject must clearly and comprehensibly describe the nature of the incident and must include at least the information and measures specified in points (b), (c), and (d) of Article 33(3) of the Regulation.
3. Notification of the data subject is not required if any of the following conditions are met:
    1. The Data Controller has implemented appropriate technical and organizational protection measures with respect to the data concerned, such as encryption, which prevents unauthorized persons from accessing the data.

2. Following the incident, the Data Controller has taken further measures that ensure the high risk to the rights and freedoms of the data subject is no longer likely to materialize.
3. Direct notification would involve disproportionate effort. In such cases, the data subjects must be informed by means of a public communication or a similarly effective measure.

4. If the Data Controller has not notified the data subject, the supervisory authority – after assessing whether the incident is likely to result in high risk – may require the Data Controller to notify the data subject or may determine that one of the conditions listed in point 3 applies.

(Based on Article 34 of the General Data Protection Regulation of the European Union)

Right to an Effective Judicial Remedy Against a Supervisory Authority

1. Without prejudice to any other administrative or non-judicial remedies, every natural and legal person has the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.
2. Without prejudice to any other administrative or non-judicial remedies, every data subject has the right to an effective judicial remedy where the supervisory authority which is competent under Articles 55 or 56 of the Regulation does not handle a complaint, or does not inform the data subject within three months of the progress or outcome of the complaint lodged under Article 77.
3. Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.
4. Where proceedings are brought against a decision of a supervisory authority which has been preceded by an opinion or a decision of the European Data Protection Board under the consistency mechanism, the supervisory authority shall forward that opinion or decision to the court.

(Based on Article 78 of the General Data Protection Regulation of the European Union)

Right to an Effective Judicial Remedy Against a Data Controller or Processor

1. Without prejudice to any available administrative or non-judicial remedies, including the right to lodge a complaint with a supervisory authority pursuant to Article 77 of the Regulation, every data subject has the right to an effective judicial remedy where they consider that their personal data has been processed in a way that does not comply with the Regulation and thereby infringes the rights guaranteed to them under the Regulation.

2. Proceedings against a Data Controller or Processor shall be brought before the courts of the Member State where the Data Controller or Processor has an establishment. However, the data subject may also bring proceedings before the courts of the Member State of their habitual residence, unless the Data Controller or Processor is a public authority of a Member State acting in the exercise of its public powers.

(Based on Article 79 of the General Data Protection Regulation of the European Union)

VIII. REMEDIES

Rights of the Data Subject in Relation to the Processing of Personal Data

1. The data subject has the right to request information about the processing of their personal data, and may request the rectification, erasure, or blocking of such data – except in cases of mandatory data processing prescribed by law – via the email address reception@hotelallora.hu, or in the manner specified for the relevant data processing activity.
2. At the request of the data subject, the Data Controller is obliged to provide information regarding:

- The personal data being processed.
- The purpose, legal basis, and duration of the processing.
- The details of any data processor (if one has been engaged).
- The circumstances, effects, and measures taken to remedy any data protection incident.
- In the case of data transfers, the legal basis, purpose, and recipients of the transfer.

3. The Data Controller is obliged to rectify or erase inaccurate personal data if:
    1. The processing is unlawful.
    2. The data subject requests it.
    3. The data is incomplete or incorrect and cannot be lawfully corrected – except where erasure is prohibited by law.
    4. The purpose of the processing has ceased, or the retention period has expired.
    5. Erasure has been ordered by a court or by the National Authority for Data Protection and Freedom of Information.
4. The Data Controller shall notify the data subject, as well as all parties to whom the data has previously been transferred, of any rectification or erasure. Notification may be omitted if it does not prejudice the legitimate interests of the data subject.

5. The data subject may object to the processing of their personal data if:
    1. The processing or transfer is solely necessary for the enforcement of the legitimate interests of the Data Controller or the recipient (except in cases of mandatory processing).
    2. The data is used for direct marketing, public opinion polling, or scientific research.
    3. The right to object is provided by law in other cases.
6. The Data Controller shall examine the objection – while suspending the processing – without delay and within no more than 15 working days, and shall inform the data subject in writing of the outcome. If the objection is justified, the Data Controller shall terminate the processing (including data collection and transfer), block the data, and notify all parties to whom the data was previously transferred.
7. If the data subject disagrees with the decision of the Data Controller, or if the Data Controller fails to meet the deadline specified in point 6, the data subject has the right to turn to the courts within 30 days.
8. Judicial enforcement: In the event of a violation of the data subject's rights, they may initiate court proceedings. The court shall hear the case out of turn. The Data Controller bears the burden of proof regarding the lawfulness of the processing.
9. In the event of a violation of the right to informational self-determination, the data subject may file a report or complaint:

Nemzeti Adatvédelmi és Információszabadság Hatóság

Address: 1125 Budapest, Szilágyi Erzsébet fasor 22/c

Phone: +36 (1) 391-1400

Fax: +36 (1) 391-1410

www: http://www.naih.hu

e-mail: ugyfelszolgalat [at] naih.hu

10. If the rights of the data subject are violated – for example, in cases involving content offensive to minors, incitement to hatred or exclusion, requests for correction, infringement of the rights of a deceased person, or violation of good reputation – the data subject may file a report or lodge a complaint:

Nemzeti Média- és Hírközlési Hatóság

1015 Budapest, Ostrom u. 23-25.

Postal address: 1525. Pf. 75

Phone: (06 1) 457 7100

Fax: (06 1) 356 5520

E-mail: info [at] nmhh.hu

IX. Other Provisions

This policy shall enter into force on December 10, 2025.