PRIVACY POLICY
ON THE RIGHTS OF THE NATURAL PERSONS CONCERNED
REGARDING THE HANDLING OF YOUR PERSONAL DATA

- supplemented by employment-related data management -

Start of validity:
May 16, 2023

Content

INTRODUCTION

This information is intended for visitors, website visitors, customers, partners, online store buyers, newsletter readers and employees of the Madame Tussauds Budapest attraction. If you are one of the Fenites, you share your personal data with us. We are responsible for their protection and safety in accordance with legal requirements. Please familiarize yourself with our information on the protection of personal data and rights under Regulation (EU) 2016/679 of the European Parliament and of the Council ("GDPR" **)** and CXII of 2011 on the right to information self-determination and freedom of information. made on the basis of Act (" **Infotv .")**

You - the reader of this information - may be referred to in this information as " **Data Subject** ", " **Data Subject** ", " **User** ", " **Customer ". Regarding his fundamental rights, the VII., VIII. and IX. chapter provides detailed information.**

Feel free to contact us with any questions, comments or complaints. The Data Controller primarily welcomes your questions, complaints, and comments **at the following e-mail address, which is specifically used for this purpose** :

adatvedelem@hungarianexperience.hu

The Data Controller reserves the right to modify this information. If the amendment affects the use of personal data provided by the Data Subject, the Data Subject will be informed of the changes by e-mail. If the details of the data management change, the Data Controller separately requests the Data Subject's consent to the changed method of data management.

CHAPTER I
NAME OF DATA PROCESSOR

The publisher of this information, also the Data Controller:

Name: Dorottya Experience Kft.
Data Protection Officer: Berecz-Fischer Petra
E-mail: adatvedelem@hungarianexperience.hu
Headquarters: 1051 Budapest, Dorottya utca 6. 2nd floor. 206.

(hereinafter: " **Data Controller** ")

These regulations can be unilaterally amended or revoked by the Data Controller at any time, with the simultaneous notification of the Data Subjects. The information is published on the Data Controller's website or, depending on the nature of the change, by direct notification to the Data Subjects.

II. CHAPTER
DATA OF VISITORS AND BUYERS

1. Registration on the website

1.1. On the website, the registrant can give his consent to the processing of his personal data by ticking the relevant box. The box is not pre-checked.

1.2. The range of personal data that can be handled: the natural person's name (surname, first name), address, telephone number, e-mail address, online identifier.

1.3. The purpose of processing personal data:
- ⇨ Fulfillment of the services provided on the website.
- ⇨ Contact via electronic, telephone or SMS inquiry.
- ⇨ Information about the Data Controller's services, contractual terms and promotions.
- ⇨ Advertising can be sent electronically or by post during the information process.
- ⇨ Analysis of website usage.

1.4. Legal basis for data management: the consent of the data subject.

1.5. Recipients of personal data and categories of recipients: employees of the Data Controller performing tasks related to customer service and marketing activities, employees of IT service providers of the Contractor as data processors.

1.6. Duration of storage of personal data: until the registration / service exists, or until the consent of the data subject is withdrawn (deletion request).

1.7. Failure to provide data results in service failure.

1.8. III. CHAPTER IV, as well as the data management arising from the issuance of invoices related to the purchase. CHAPTER provides further information.

2. Visitor data management on the website

2.1. accordance with common Internet practice, the Data Controller may also use cookies on its website. You can find more information about the cookie settings currently used by the data controller in the " **Cookie Settings " document on the website.**

A cookie is a small file containing a string of characters that is placed on a visitor's computer when they visit a website . When you visit the website again , thanks to the cookie, the website can recognize the visitor's browser. Cookies can store user settings (e.g. selected language) and other information. Among other things, they collect information about the visitor and his device, remember the visitor's individual settings, and can be used, e.g. when using online shopping carts. In general, cookies facilitate the use of the website, help the website to provide users with a real web experience and be an effective source of information, and also ensure that the website operator can control the operation of the website, prevent abuses and ensure that the services provided on the website are undisturbed and of an adequate standard .

2.2. During the first visit to the website, the Data Subject receives information about cookies in the form of a short summary, during which more information is available on a link in this Privacy Policy and in the Cookie Settings documents.

2.3. During the use of the website, the website of the Data Controller records and manages the following data about the visitor and the device used for browsing:

- ⇨ the IP address used by the visitor,
- ⇨ browser type,
- ⇨ characteristics of the operating system of the device used for browsing (set language),
- ⇨ date of visit,
- ⇨ the visited (sub)page, function or service.

2.4. Accepting and authorizing the use of cookies is not mandatory. You can reset your browser settings to reject all cookies or to indicate when a cookie is currently being sent. Although most browsers automatically accept cookies by default , they can usually be changed to prevent automatic acceptance and offer a choice each time.

You can find information about the cookie settings of the most popular browsers at the following links:

- ⇨ Google Chrome: https://support.google.com/accounts/answer/61416?hl=en
- ⇨ Firefox: https://support.mozilla.org/hu/kb/sutik-engedelizeze-es-tiltasa-amit-weboldak-haszn
- ⇨ Microsoft Internet Explorer 11: http://windows.microsoft.com/hu-hu/internet-explorer/delete-manage-cookies#ie=ie-11
- ⇨ Microsoft Internet Explorer 10: http://windows.microsoft.com/hu-hu/internet-explorer/delete-manage-cookies#ie=ie-10-win-7
- ⇨ Microsoft Internet Explorer 9: http://windows.microsoft.com/hu-hu/internet-explorer/delete-manage-cookies#ie=ie-9

- ⇨ Microsoft Internet Explorer 8: http://windows.microsoft.com/hu-hu/internet-explorer/delete-manage-cookies#ie=ie-8
- ⇨ Microsoft Edge: http://windows.microsoft.com/hu-hu/windows-10/edge-privacy-faq
- ⇨ Safari : https://support.apple.com/hu-hu/HT201265

In addition to all this, we would like to point out that certain website functions or services may not work properly without cookies .

2.5. The cookies used on the website are not in themselves suitable for identifying the user.

2.6. Cookies used on the website of the Data Controller :

2.6.1. Technically essential session cookies:

These cookies are necessary so that visitors can browse the website, use its functions smoothly and fully, the services available through the website, so - among others - in particular, the comments of the actions performed by the visitor on the given pages during a visit. The duration of the data management of these cookies applies only to the visitor's current visit, this type of cookie is automatically deleted from the computer when the session ends or when the browser is closed.
The managed data range: AVChatUserId , JSESSIONID, portal referee .
The legal basis for this data management is Act CVIII of 2001 on certain issues of electronic commercial services and information society services. Act (Elkertv .) 13/A. Section (3), legitimate interest.
The purpose of data management is to ensure the proper functioning of the website.
Duration of data management: 1 year from the date of data collection

2.6.2. Cookies requiring consent:

These provide an opportunity for the Data Controller to remember the user's website-related choices. The visitor can prohibit this data management at any time before using the service and during the use of the service. These data cannot be linked to the user's identification data and cannot be transferred to third parties without the user's consent.

The legal basis for data management is the visitor's consent.
Purpose of data management: Increasing the efficiency of the service, increasing the user experience, making the use of the website more convenient.
Duration of data management: withdrawal of consent, or see the links indicated in the points below.

2.6.2.1. Cookies that facilitate use

2.6.2.2. Performance cookies:

Google Analytics cookies - you can find information about this here: https://developers.google.com/analytics/devguides/collection/analyticsjs/cookie-usage

Google AdWords cookies - you can find information about this here: https://support.google.com/adwords/answer/2407785?hl=en

Microsoft Clarity cookies - you can find information about this here: https://learn.microsoft.com/en-us/clarity/cookie-list

2.6.2.3 Cookies for marketing purposes:

Scope of managed data: user IP address, access path to the website (page viewed before the website, page visited through the website), time of visit to the website, duration of visit to the website, browser ID, location of the website visit, http headers (information about the web browser , page location, document, referrer and person using the website), pixel-specific data (Pixel ID and

Facebook cookie), button click data (includes all buttons clicked by website visitors, button labels and visits as a result of button clicks pages).

Purpose of data management: Marketing cookies are used by the data controller to monitor website activity of visitors. Its purpose is to serve relevant ads to individual users and encourage them to engage, making the website more valuable to content publishers and third-party advertisers. The purpose of their use is to learn about the interests of users and to display personalized advertising content on the website and - after leaving the page - on the websites of third parties.

Legal basis for data management: Statistical cookies are managed by the Data Controller on the basis of Article 6 (1) point a) of the GDPR (consent of the data subject), which consent is given by the data subject upon the first visit to the page by ticking the checkboxes in the pop-up window.

Information about the duration of data storage:

Google's general cookie information:
https://www.google.com/policies/technologies/types/
Google Analytics information:
https://developers.google.com/analytics/devguides/collection/analyticsjs/cookie-usage?hl=en
Facebook information:
https://www.facebook.com/ads/preferences/?entry_product=ad_settings_screen

Google Tag Manager

Google Tag Manager is a Google Inc., 1600 Amphitheater Parkway , Mountain View , CA 94043, USA (“Google”) is a service that allows you to create, update and manage tags (tags). Tags are small pieces of code on our website that are used, among other things, to measure traffic and visitor behavior and to determine the impact of online advertising and social channels. When you visit our website, the current tag configuration is sent to your browser. In this way, you will receive instructions on which tags to activate. The tool itself does not collect any personal data, but ensures the activation of other tags that may in turn collect data. More information on the operation of Google Tag Manager can be found at the following link:
https://support.google.com/tagmanager/answer/6102821?hl=en

Google Inc. remarketing or "Similar Audiences" functionality

Data controller A is used by Google Inc., 1600 Amphitheater Parkway , Mountain View , CA 94043, USA (“Google”) remarketing or “Similar Audiences” function. This function enables the data controller to offer website visitors targeted advertising by placing personalized, interest-based ads for website visitors when they visit other websites within the Google Display Network. Google uses cookies to analyze the use of the website, and the creation of interest-based ads is based on this. For this purpose, Google stores a small file containing a series of numbers in the browsers of website visitors. Visits to the website and anonymized data about the use of the website are collected through this number. The personal data of website visitors is not usually stored. If you visit another website within the Google Display Network, you will be shown ads that most likely take into account the previously selected product and information areas. More information about Google Remarketing and Google's Privacy Policy can be found here: https://policies.google.com/technologies/ads

Facebook pixel

The Facebook pixel is Meta Platforms Service of Ireland Limited (formerly Facebook Ireland Limited). This is a piece of code placed on our site that enables users registered and logged in on Facebook to track and analyze

visitor activity related to our site, as well as collect remarketing opportunities based on your interests. As a data controller, we can evaluate and optimize our advertisements with the help of the data obtained in this way, and provide personalized offers to the visitors of our website and to specific groups of visitors. You can read Facebook's data management policy here: https://www.facebook.com/privacy/explanation

3. Data management related to the newsletter service

3.1. On the website, natural persons registering for the newsletter service can give their consent to the processing of their personal data by checking the relevant box. The box is not pre-checked. The person concerned can unsubscribe from the newsletter at any time by using the "Unsubscribe" application of the newsletter, or by making a statement in writing or by e-mail, which means withdrawal of consent. In such a case, all data of the unsubscriber must be deleted immediately.

3.2. The range of personal data that can be processed: the natural person's name (surname, first name), e-mail address.

3.3. The purpose of processing personal data:
- ⇨ Sending a newsletter about the Data Controller's products and services
- ⇨ Satisfaction survey
- ⇨ Sending advertising material

3.4. Legal basis for data management: the consent of the data subject.

3.5. Recipients of personal data and categories of recipients: employees of the Data Controller performing tasks related to customer service and marketing activities, employees of the Data Controller's IT service providers as data processors for the purpose of providing hosting services.

3.6. Duration of storage of personal data: until the existence of the newsletter service, or until the consent of the data subject is withdrawn (deletion request). Failure to provide data makes access to current offers difficult.

4. Community guidelines / Data management on Facebook, Instagram

4.1. The Data Controller maintains a Facebook and Instagram page for the purpose of introducing and promoting its services and products. A question asked on the Data Controller's Facebook or Instagram page is not considered an officially submitted complaint. Please direct your inquiries of this kind to DOROTTYA EXPERIENCE KFT. Address: Apáczai Csere János utca 15/2. 1051 Budapest , comments and complaints about data management to **adatvedelem@hungarianexperience.hu** please send it to

4.2. Personal data published by visitors on the Data Controller's Facebook or Instagram pages is not managed by the Data Controller.

4.3. Visitors are governed by Facebook's Privacy and Terms of Service.

4.4. In case of publication of illegal or offensive content, the Data Controller may exclude the person concerned from membership or delete his/her comment without prior notice.

4.5. The Data Controller is not responsible for data content and comments published by Facebook or Instagram users that violate the law. The Data Controller is not responsible for any errors, malfunctions or problems arising from changes to the operation of the system resulting from the operation of Facebook or Instagram.

5. Data management related to evaluations, feedback and complaints

5.1. The legal basis for data processing during data processing in the complaint book or customer book in the z Data Controller's own commercial unit is: legal obligation .

5.1.1. Scope of processed data: name; address, telephone number, e-mail address, signature

5.1.2. The purpose of processing personal data:
- ⇨ investigation of customer complaints, thereby improving the quality of the service

5.1.3. Legal basis for data management: legal obligation (Article 5 (4) of Act CLXIV of 2005 on trade)

5.1.4. Recipients of personal data and categories of recipients: employees of the Data Controller performing tasks related to customer service.

5.1.5. Duration of storage of personal data: 3 years from the date of the complaint (1997 CLV. Act § 17/A. Paragraph (7)).

5.1.6. Failure to provide data makes it difficult or impossible to assess the complaint or provide information on the outcome of the assessment.

5.2. If the Data Subjects wish to contact the Data Controller with feedback, complaints or comments that are not to be recorded in the complaint book contained in point 5.1, they should primarily do so via the dedicated devices located in the attraction, or through the The Data Controller is waiting for you at info@hungarianexperience.hu .

Based on the legitimate interests of the Data Controller, it carries out data management activities in relation to feedback and complaints made by visitors in relation to the attraction or activities carried out in the area of interest of any Data Controller.

Interest assessment test : In relation to the relevant legal regulations, the jurisprudence of the National Data Protection Authority (the resolutions adopted under the case numbers NAIH/ 2018/2570/2/V and NAIH/2016/1684/2/V), as well as the previously effective processing of personal data, individuals Data Protection Working Group 6/2014 established on the basis of Article 29 of Directive 95/46/EC of the European Parliament and of the Council on data protection and the free flow of such data. Based on its Opinion no., the Data Controller carried out a consideration of interests in relation to the data management activity contained in point 5.2 above, as summarized below.

Scope of stakeholders: all natural persons who send feedback, complaints, and comments regarding the service provided by the Data Controller to the Data Controller.

Nature of data management: collection, recording, organization and use of personal data in order to improve the service.

The purpose of data management is: quality assurance, increasing the quality of the service provided by the Data Controller and the satisfaction of customers and visitors. Failure to provide data makes it difficult to measure satisfaction.

Lawfulness of data management: The Data Controller carries out the data management activities recorded above for its own legitimate interests. About consumer protection CLV of 1997. the law defines the requirements for the method of handling complaints, the requirement for the possibility to file a complaint, the existence of a legitimate interest can therefore also be determined **from the legal regulations** .

Legitimate interest: The Data Controller provides its services to visitors and customers, with the aim of realizing economic benefits during this activity. In order for the Data Controller's customers to be able to decide with greater certainty whether they want to use the Data Controller's services, they can express their satisfaction or dissatisfaction with the Data Controller, thus creating useful information for other customers, thereby increasing user satisfaction related to the services provided by the Data Controller , ultimately increasing the number of potential satisfied users and thereby promoting the economic interests of the Data Controller, it is necessary for customers to provide evaluations of the service provided by the Data Controller.

Necessity of data management: The above-defined data management is absolutely **necessary, suitable and proportionate to achieve the interest** . The above goals cannot be achieved in any other way than the submission of personal evaluations and opinions, there is no suitable way for the Data Controller to evaluate information from a wide range of impartial persons apart from this data management in a way that is less intrusive on the Data Subject's privacy. The possibility to file a complaint is about consumer protection CLV of 1997. required by law.

The legitimate interest determined by the Data Controller is sufficiently **clear** and precisely defined. The Data Controller has a business and economic interest in protecting the interest, and this interest is also protected by law, so it is **a real, existing interest** of the Data Controller .

In relation to this data management activity, customers and visitors can decide for themselves whether or not they wish to submit an evaluation or complaint. If a customer or visitor does not wish to submit an evaluation, no personal data relating to him will be generated from the point of view of this data management, and therefore he will not be affected from the point of view of this point of the balance of interests test.

The fact that the users of the platforms maintained by the Data Controller have the opportunity to submit an evaluation is also useful for them, as this means that either they themselves or other users can benefit from a higher quality service in the future.

In contrast to the advantages that also appear on the side of the Data Subjects, the legal disadvantage caused to the Data Subjects by the data management consists in the fact that the information created by them (the submitted evaluation) is kept by the Data Controller as personal data for 3 years (CLV. Act of 1997 § 17/A. (7) paragraph) , during which time the data subject can subsequently reevaluate his previous position or his intention to make his opinion available.

The enforcement of the legitimate interest of the Data Controller - taking into account the method of creation of personal data (information produced by customers, which the customers themselves write and submit on a voluntary basis) - definitely exceeds any potential disadvantages caused to customers and visitors. Taking into account the fact that submitting an evaluation is not mandatory for customers and visitors, but only an option, so there is no balance between the legitimate interest of the Data Controller and the legal disadvantage resulting from the management of the customers' personal data, the legitimate interest of the Data Controller exceeds the minor legal disadvantage caused to the customers.

In order to protect the interests of the data subjects, the Data Controller processes the personal data for a limited period of time and deletes the personal data within 3 years, so the legitimate interest of the Contractor continues to exceed the minor legal disadvantage caused to the data subjects.

Transparency: The Data Controller sends information to the data subject to the specified e-mail address about the data management, its circumstances, the purpose and duration of the data management, the rights of the Data Subjects, the measures for data protection, and the contact details of the data protection officer. The information provided by the Data Controller covers the purposes for which the processing of the data subject's data is possible. The data subject has the right to access the data collected for the purpose of contact, and to exercise this right simply and at reasonable intervals in order to establish and check the legality of the data management. Given that the purpose of the data management can really be achieved, the Data Controller ensures that the data subject can specify the personal data concerning him and that the Data Controller corrects them without delay. The data controller shall inform the data subject without undue delay if a data protection incident occurs with regard to the processed personal data, and it is likely to involve a high risk for the rights and freedoms of natural persons, in order to enable the data subject to take the necessary precautions.

The Data Controller makes this interest assessment test available to the Data Subjects on its own website, as well as informs the Data Subjects in detail about its data management activities, the Data Subjects' rights and legal remedies.

The result of the consideration of interests:

Pursuant to the above interest balancing test, the Data Controller is entitled to conduct data management activities related to evaluations, complaints, and feedback submitted by customers, visitors, as Data Subjects, based on its legitimate interest, given that the Data Controller's legitimate interest outweighs any potential disadvantages to customers through data management. Necessary and proportionate data processing is carried out in accordance with the reasonable expectations of the data subject, i.e
In addition to the necessary administrative protection measures established by the data controller, there is no high risk for the rights and freedoms of the affected persons.

6. Data management related to the camera system

6.1. In our company's rooms open to visitors, service rooms, and warehouses, human life, physical integrity, personal freedom, the protection of business secrets and the protection of assets, in order to prevent and detect violations of the law, to convict the perpetrator, and to prove the violations of the law, it uses an electronic surveillance system that also enables image recording, on the basis of which it can consider the image and behavior of the person concerned, which is recorded by the camera, as personal data .

6.2. The legal basis for this data management is the enforcement of the legitimate interests of the employer.

6.3. A warning sign and information about the fact of the application of the electronic monitoring system in a given area was placed in a clearly visible place, in a way that helps third parties who wish to appear in the area to find their way around. The information is to be understood in relation to each room, it is indicated in several places when entering the Attraction.

6.4. The recordings will be kept for a maximum of 3 (three) working days if they are not used. Use is considered if the recorded image, sound, or image and sound recording, as well as other personal data, is intended to be used as evidence in court or other official proceedings. In the latter case, the time of retention is the date of the legally binding end of the official or court proceedings.

6.5. Information about data storage: the recordings are stored separately on the server located at the headquarters of the Data Controller, thus ensuring that unauthorized persons cannot view and copy the recordings.

6.6. Access to the recordings: the administrator of the Data Controller, the employer of the employees in the given area, those authorized by law and the security guard are entitled to view the current images of the cameras, and the administrator of the Data Controller is authorized to view the recordings and record them on a data carrier in order to achieve the data management goals indicated in this information. . Logging: the Data Controller records the access to recorded recordings and recordings on data media with the name of the person performing it, the reason for learning the data and the date of the data.

6.7. The person whose right or legitimate interest is affected by the recording of the image, sound, or image and sound recording data may, within three working days from the recording of the image, sound, and image and sound recording, request, by proving his right or legitimate interest, that the data should not be destroyed or deleted by its manager.

6.8. In addition to those authorized to do so by law, the management staff, the employer's manager and deputy, as well as the workplace manager of the monitored area are entitled to view the data recorded by the electronic monitoring system for the purpose of revealing violations and checking the operation of the system.

6.9. Cameras placed in the rooms of the Attraction accessible to visitors: Admission Zone (2 pcs), Budapest Corso (2 pcs), Epic Encounter (2 pcs), toilet hall (no toilet) (2 pcs), Hungarian Spirit (8 pcs), Café (3 pcs), Fashion (2 pcs), Movie (2 pcs), Music (2 pcs), Sport (2 pcs), VIP Party (2 pcs), How lake Make it (2pcs), Shop (2pcs)

7. Discounted ticket purchase

7.1. If the Data Subject wishes to take advantage of a discount that entitles him to reduced entry, he must provide the following personal data to prove his entitlement to the discount (scope of personal data that can be processed): name, photograph of the natural person, characteristics entitling him to reduced entry (age or disability), the number of your appropriate disability card.

7.2. The purpose of processing personal data is to check the legitimacy of the use of the discount.

7.3. Legal basis for data management: the consent of the data subject.

7.4. Recipients of personal data and categories of recipients: employees of the Data Controller who are responsible for entry.

7.5. Duration of storage of personal data: personal data is not stored by the Data Controller.

7.6. Failure to provide data will result in the Visitor not being entitled to use the discount.

III. CHAPTER
DATA OF PARTNERS AND LEGAL ENTITY CUSTOMERS

8. Management of contractual partners' data

8.1. mother's name, place and time of birth, tax identification number, registered office of the natural person contracted with it as a supplier, agent, contractor, seller, or other similar partner for the purpose of concluding, fulfilling, terminating the contract, and providing contractual benefits. , location address, telephone number, e-mail address, bank account number, sole proprietorship registration number, and in the case of a recording for promotional purposes, the image of the partner. This data management is considered legal even if the data management is necessary to take steps at the request of the data subject prior to the conclusion of the contract.

8.2. The data management is based on the legal title of the performance of the contract in the case of data that is absolutely necessary for the performance of the contract. The data management is based on a legal obligation regarding the data that is necessary for issuing invoices. Data processing is based on the consent of the data subject regarding the telephone number and e-mail address. The legal title of the data management is the legitimate interest of the data controller in the case of the data necessary to assert any claim (mother's name, place of birth, time).

8.3. Recipients of personal data: employees of the Data Controller performing tasks related to contractual relations, employees performing accounting and taxation tasks, and its accounting service provider as a data processor.

8.4. Duration of processing personal data: 5 years after the termination of the contract, 5 years in the case of the telephone number and e-mail address, or the withdrawal of the consent of the person concerned.

8.5. Failure to provide data makes it impossible to provide the service.

9. Contact details of clients, partners and representatives of natural persons

9.1. The range of personal data that can be handled: the name, address, telephone number, e-mail address of the natural person.

9.2. The purpose of processing personal data: fulfillment of the contract concluded with the Data Controller's legal entity partner, business relationship, legal basis: consent of the data subject.

9.3. Recipients of personal data and categories of recipients: employees of the Data Controller performing tasks related to contractual relations.

9.4. Duration of storage of personal data: for 5 years after the existence of the business relationship or the quality of representative of the person concerned.

9.5. Failure to provide data makes it impossible to provide the service.

ARC. CHAPTER
DATA MANAGEMENT RELATED TO EMPLOYMENT

10. Labor and personnel records

10.1. Only such data may be requested and kept on record from employees, as well as occupational medical suitability tests, which are necessary for the establishment, maintenance and termination of employment, as well as for the provision of social welfare benefits and which do not infringe the employee's personal rights. Present IV. Sections 10, 12, and 17 of this chapter specifically apply to data management related to working school cooperative members.

10.2. As an employer, the Data Controller manages the following employee data:

Managed data	Data management title	Purpose of data management
Name	Data management is necessary to fulfill the contract or to take steps at the request of the data subject prior to the conclusion of the contract [Article 6(1)(b) GDPR]	Establishment , performance, termination of an employment relationship.
Birth name		
Date of birth		
Place of birth		
His mother's name		
Address, place of residence		
Nationality		
Bank account number		
Identity card number (view only)		
the official ID card confirming the legal address (viewing only)		
The method and reasons for terminating the employment relationship		
In the case of a foreign employee, the name and number of the document certifying the right to work,		
Phone number		
E-mail address		
Job description		
Wages		
Working hours		
Workplace		
Work order		
Data on professional qualifications		
Data on professional experience		
Document proving your education and professional qualifications (viewing only)		

Evaluation of the employee's work		
Tax identification number	Data management is necessary to fulfill the legal obligation of the data controller [GDPR Article 6 (1) point c)]	Compliance with legal obligations.
Social security number		
Pensioner identification number (in the case of a retired employee)		
Debt to be deducted from the employee's salary based on a legally binding decision or legislation, and the right to do so		
Data recorded in the records of accidents involving employees		
Summary of job suitability tests		
Patient data		
Leave data		
Name, place and date of birth of children under 16 (if the employee wishes to take parental leave)		
In the case of private pension fund and voluntary mutual insurance fund membership, the name of the fund, its identification number and the employee's membership number		
Camera and access control system used by the data controller for security and property protection purposes, and data recorded by positioning systems	Legitimate interest of the employer [GDPR Article 6 (1) point f)]	Security and asset protection

10.3. The purpose of processing personal data is: conclusion, fulfillment of employment contracts, employment.

10.4. Recipients of personal data: the manager authorized to exercise employer rights at the Data Controller, the Data Controller's employees and data processors performing labor tasks , especially the service provider providing bookkeeping, payroll, and social security services.

10.5. Duration of storage of personal data: 3 years after termination of employment.

10.6. Failure to provide data may result in the non-establishment of the legal relationship and the termination of the employment contract.

11. Data management related to aptitude tests

11.1. The employee can only be subject to an aptitude test that is prescribed by a rule relating to an employment relationship, or which is necessary in order to exercise a right or fulfill an obligation defined in a rule relating to an employment relationship. Before the test, the employee receives information about, among other things, what kind of skills and abilities the aptitude test is aimed at assessing, and what tool and method the test is carried out with. If legislation requires the examination to be carried out, the employee will also receive information on the exact designation of the legislation.

11.2. The range of personal data that can be handled: the fact of job suitability and the conditions necessary for this.

11.3. Legal basis for data management: legal obligation.

11.4. The purpose of processing personal data is: establishing and maintaining an employment relationship, filling a position.

11.5. Recipients of personal data and categories of recipients: the results of the examination can be seen by the examined employees and the specialist conducting the examination. The employer can only receive information on whether the examined person is suitable for the job or not, and what conditions must be provided for this. The details of the investigation and its complete documentation are not known to the employer.

11.6. Duration of processing personal data: 3 years after termination of employment.

11.7. Failure to provide data may result in the non-establishment of the legal relationship and the termination of the employment contract.

12. Management of the data of employees applying for recruitment, applications, resumes

12.1. The range of personal data that can be processed: name of the natural person, qualification data, telephone number, e-mail address, previous employer's record of the applicant (if any).

12.2. The purpose of processing personal data is to evaluate applications and tenders. The person concerned will be informed if the employer did not choose him/her for the given job.

12.3. Legal basis for data management: as stated in point 8.2.

12.4. Recipients of personal data and categories of recipients: manager authorized to exercise employer rights at the Data Controller, employees of the Data Controller performing labor duties .

12.5. Duration of storage of personal data: until the application or tender is evaluated. The personal data of applicants who are not selected, as well as the data of those who have withdrawn their application, will be deleted by the Data Controller.

12.6. The employer may only retain the applications based on the specific, clear and voluntary consent of the person concerned, provided that their retention is necessary in order to achieve the purpose of data management in accordance with the law. The applicant can give this consent after the admission procedure has been completed. In this case, the purpose of data management is the possible establishment of a future employment relationship, the legal basis of data management is the consent of the data subject, the recipients are the persons listed in point 10.4, and the duration is 6 months, or the withdrawal of the consent of the data subject.

12.7. Failure to provide data may result in the non-establishment of the legal relationship and the termination of the employment contract.

13. Data management related to checking the use of e-mail accounts

13.1. If the Data Controller provides an e-mail account to the employee, the employee can use this e-mail address and account exclusively for the purpose of his job duties, in order for the employees to keep in touch with each other or to correspond with clients and other persons on behalf of the employer. , with organizations.

13.2. The employee may not use the e-mail account for personal purposes, and may not store personal mail in the account.

13.3. The employer is entitled to check the entire content and use of the e-mail account regularly – every 3 months – and the legal basis for data management is the legitimate interest of the employer. The purpose of the inspection is to verify compliance with the employer's provision regarding the use of the e-mail account, as well as to verify the employee's obligations.

13.4. The manager of the employer or the practitioner of employer rights is entitled to the inspection.

13.5. The employee may be present during the inspection.

13.6. Before the inspection, the employee receives information about the employer's interest in the inspection, who can carry out the inspection on behalf of the employer, according to which rules the inspection can take place (adherence to the principle of gradualism) and what the

procedure is, what rights and remedies are available to the employee regarding the data management associated with the verification of the e-mail account.

13.7. During the inspection, the principle of gradation must be applied, so it must first be established from the address and subject of the e-mail that it is related to the employee's job duties and not for personal purposes. The employer may examine the content of e-mails for non-personal purposes without restriction.

13.8. If, contrary to the provisions of these regulations, it can be established that the employee used the e-mail account for personal purposes, the employee must be asked to delete the personal data immediately. In the event of the employee's absence or lack of cooperation, the employer will delete the personal data during the inspection. Due to the use of the e-mail account contrary to these regulations, the employer may apply labor law legal consequences to the employee.

13.9. The employee may use the rights described in the chapter on the rights of the data subject of these regulations in connection with the data management associated with the control of the e-mail account.

14. Data management related to the control of Internet use at work

14.1. On the devices provided by the employer, the employee can only view websites related to his job duties, the employer prohibits the use of the internet at work for personal purposes.

14.2. As a job task, the Data Controller is the authorized person for internet registrations carried out on behalf of the Data Controller, and during registration, the identifier and password referring to the company must be used. The employee may not use personal data as a password or username. If the provision of personal data is also required for registration, the Data Controller initiates their deletion when the employment relationship is terminated.

14.3. The employer can control the employee's use of the Internet at work, which is governed by the provisions of point 11 and its legal consequences.

15. Data management related to the control of computers, laptops and tablets

15.1. The employee may only use the computer, laptop, or tablet provided by the Data Controller for the purpose of work for the performance of his job duties, the Data Controller does not permit their use for private purposes, and the employee may not manage or store any personal data or correspondence on these devices. The employer can check data stored on these devices.

15.2. The employee may not use personal data or identification based on fingerprints or facial recognition as a password or access code.

15.3. The control and legal consequences of these devices by the employer are otherwise governed by the provisions of point 11.

16. Data management related to monitoring the use of company mobile phones

16.1. The employer does not allow the use of the company mobile phone for private purposes, the mobile phone can only be used for work-related purposes, and the employer can check the phone number and data of all outgoing calls, as well as the data stored on the mobile phone.

16.2. The employee must notify the employer if the company mobile phone is used for private purposes. In this case, the control can be carried out by the employer requesting a call log from the telephone service provider and asking the employee to make the numbers called unrecognizable on the document for private calls. The employer can stipulate that the costs of calls for private purposes are borne by the employee.

16.3. The employee may not use personal data or identification based on fingerprints or facial recognition as a password or access code.

16.4. In other respects, the inspection and its legal consequences are governed by the provisions of point 11.

17. Data management related to the camera system

17.1. In our company's rooms open to visitors, service rooms, and warehouses, human life, physical integrity, personal freedom, the protection of business secrets and the protection of assets, in order to prevent and detect violations of the law, to convict the perpetrator, and to prove the violations of the law, it uses an electronic surveillance system that also enables image recording, on the basis of which it can consider the image and behavior of the person concerned, which is recorded by the camera, as personal data .

17.2. The legal basis for this data management is the enforcement of the legitimate interests of the employer.

17.3. A warning sign and information about the fact of the application of the electronic surveillance system in a given area has been placed in a clearly visible place, in a way that facilitates the orientation of third parties who wish to appear in the area. The information is to be understood in relation to each room, it is indicated in several places when entering the Attraction.

17.4. The recordings will be kept for a maximum of 3 (three) working days if they are not used. Use is considered if the recorded image, sound, or image and sound recording, as well as other personal data, is intended to be used as evidence in court or other official proceedings. In the latter case, the time of retention is the date of the legally binding end of the official or court proceedings.

17.5. Information about data storage: the recordings are stored separately on the server located at the headquarters of the Data Controller, thus ensuring that unauthorized persons cannot view and copy the recordings.

17.6. Access to the recordings: to view the current image of the cameras, the manager of the Data Controller, the employer of the employees in the given area, those authorized by law and the security guard, and the manager of the Data Controller is entitled to view the recordings and record them on a data carrier in order to achieve the data management goals indicated in this information. . Logging: the Data Controller records the access to recorded recordings and recordings on data media with the name of the person performing it, the reason for learning the data and the date of the data.

17.7. The person whose right or legitimate interest is affected by the recording of the data of the image, sound, or image and sound recording may, within three working days from the recording of the image, sound, and image and sound recording, request, by proving his right or legitimate interest, that the data should not be destroyed or deleted by its manager.

17.8. Cameras placed in the Attraction: Admission Zone (2 pcs), Budapest Corso (2 pcs), Epic Encounter (2 pcs), toilet hall (no toilet) (2 pcs), Hungarian Spirit (8 pcs), Café (3 pcs), Café warehouse (1 pcs), Fashion (2 pcs), Movie (2 pcs), Music (2 pcs), Sport (2 pcs), VIP Party (2 pcs), How lake Make it (2 pcs), Shop (4 pcs), Figure service room (1 pc), Cellar corridor (2 pcs), Cash container warehouse (1 pc).

CHAPTER V
DATA PROCESSING BASED ON LEGAL OBLIGATION

18. Data management for the purpose of fulfilling tax and accounting obligations

18.1. The Data Controller manages the legally defined data of natural persons entering into business relations with it as a buyer or supplier for the purpose of fulfilling legal obligations, tax and accounting obligations prescribed by law (bookkeeping, taxation). The processed data is in accordance with Article CXXVII of 2007 on general sales tax. TV. based on § 169, in particular: tax number, name, address, tax status, based on § 167 of Act C of 2000 on accounting: name, address, designation of the person or organization ordering the economic transaction, the voucher issuer and the the signature of the person certifying the implementation of the provision and, depending on the organization, the inspector; the signature of the receiver on the stock movement receipts and money management receipts,

and the payer's signature on the receipts, CXVII of 1995 on personal income tax. based on the law: entrepreneur ID number, primary producer ID number, tax identification number.

18.2. The purpose of processing personal data is to fulfill tax and accounting obligations.

18.3. Legal basis for data management: fulfillment of a legal obligation.

18.4. The period of storage of personal data is 8 years after the termination of the legal relationship providing the legal basis.

18.5. Recipients of personal data: the Data Controller's employees and data processors performing tax, bookkeeping, payroll, and social security tasks.

18.6. Failure to provide data results in the non-establishment of the legal relationship.

VI. CHAPTER
NAME OF DATA PROCESSORS

Data processor: a natural or legal person, public authority, agency or any other body that processes personal data on behalf of the data controller (GDPR Article 4, 8). The Data Processors carry out the data management according to the instructions of the Data Controller, they cannot make substantive decisions regarding data management, they can only process the personal data they come to know in accordance with the provisions of the Data Controller, they cannot perform data processing for their own purposes, and they are also obliged to store and preserve the personal data in accordance with the provisions of the Data Controller.

19. IT service providers of the Data Controller

19.1. For the maintenance and management of its website, the Data Controller uses data processors who provide IT services and hosting services, and within the framework of this - for the duration of the contract with them - manage the personal data provided on the website.

19.2. The data processors are named as follows:

Purpose of personal data management: website operation
Company name: Fribbit Kft.
Headquarters: 2040 Budaörs, Templom tér 19.
Company registration number: 13 09 176238
Tax number: 25325616-2-13
Representative: Richard Pétercsák
Phone number: +36 30 4736966
Fax: -
Email: richard@fribbit.com
Website: www.fribbit.com

Purpose of personal data management: operation of the company's management system
Company name: FITS Magyarország Kft.
Headquarters: 8600 Siófok, Szent László utca 89/A fsz. 3.
Company registration number: 14 09 313460
Tax number: 13908740-2-14
Representative: Tamás Munkácsy
Phone number: +36 30 203 3777
Fax: -
E-mail address: tamas.munkacsy@fits.hu
Website: www.fits.hu

Purpose of processing personal data: sending a newsletter
Company Name: Mailchimp c/o The rocket Science Group, LLC
Headquarters: 675 Ponce De Leon Ave NE Suite 5000 Atlanta, GA 30308 USA
Tax number: MOSS NO. 372008134
Phone number: +1 800 315-5939
Website: www.mailchimp.com

Information according to Article 14, paragraph (1) point f) GDPR:
In the absence of a compliance decision, the data processor applies general data protection clauses approved by the European Commission, which are considered adequate data management guarantees under the GDPR. More information on this is available at the following links:
https://mailchimp.com/legal/data-processing-addendum/
https://mailchimp.com/help/mailchimp-european-data-transfers/

Purpose of processing personal data: cash register system operation
Company name: Banktech Safe Kft.
Headquarters: 1124 Budapest, Hegyalja út 154.
Company registration number: 01 09 362591
Tax number: 10948448243
Representative: Ferenc Vásony
Phone number: +3630-471-5312

Purpose of processing personal data: hosting service
Company name: Microsoft Ireland Operations Limited (Microsoft Cloud and Azure Services)
Headquarters: 70 Sir Rogerson's Quay , Dublin 2, Ireland
Address: One Microsoft Place , South County Business Park, Leopardstown , Dublin 18, Ireland
Company registration number: 256796
Tax number: IE8256796U
Phone number: +353 (0) 1 295 3826; +1 800 710 200
Website: https://azure.microsoft.com/hu-hu/

Purpose of processing personal data: conducting online banking transactions
Hungarian Branch Office of Worldline Financial Services (Europe) SA
Headquarters: 1117 Budapest, Budafoki út 91-93. C. intact. fst.
Address: 1034 Budapest, Tímár utca 20. 4th floor.
Company registration number: 01-17-000672
Tax number: 23106554-2-41
Email: info.hu@six-payment-services.com
Phone number: +36 1 490 0234
Website: https://www.six-payment-services.com/hu/shared/contacts/customer-care/customer-care-hu.html

Purpose of processing personal data: analysis of website visitors in order to increase the user experience and improve the quality of the service provided by the Data Controller
Company name: sxm -Network Kft.
Headquarters: 2636 Tésa, Petőfi utca 16.
Address: 1116 Budapest, Barázda utca 42. 3rd floor.
Company registration number: 13-09-144010
Tax number: 23127584-2-13
E-mail: hello@adamic.hu
Website: https://adamic.hu/

20. The Data Controller's accounting service provider

20.1. In order to fulfill its tax and accounting obligations, the Data Controller uses an external service provider with an accounting service contract, who also manages the personal data of natural persons who have a contract or payment relationship with the Data Controller, for the purpose of fulfilling the tax and accounting obligations of the Data Controller.

20.2. The name of the data processor is as follows:

Company name: KBOSS.hu Kft.
Headquarters: 1031 Budapest, Záhony utca 7.
Company registration number: 01-09-303201
Tax number: 13421739-2-41
Representative: Balázs Ángyan, managing director
E-mail address: info@szamlazz.hu
Website: www.szamlazz.hu

Purpose of processing personal data: checking camera footage for health and property protection purposes
Company name: Defense System Kft.
Headquarters: 1051 Budapest, Dorottya utca 6. 5th em. Door 509
Address: 1051 Budapest, Dorottya utca 6. 5th floor. Door 509
Company registration number: 01-09-309785
Tax number: 25440506-2-41
E-mail: pisak.laszlo@dsystem.hu
Website: https://dsystem.hu/

21. The Data Controller's service provider related to the delivery of goods

21.1. Magyar Posta Zrt. cooperates in the delivery of the ordered goods on the basis of a written contract concluded with the Data Controller. In doing so, Magyar Posta Zrt. may process the customer's name, address and telephone number until the delivery of the ordered goods, after which it will be deleted immediately.

Company name: Magyar Posta Zrt.
Headquarters: 1138 Budapest, Dunavirág utca 2-6.
Company registration number: 01-10-042463
Tax number: 10901232-2-44
Representative: Balázs Ángyan, managing director
Telephone: +36-40-464-646; +36-1-767-8200
E-mail address: ugyfelszolgalat@posta.hu
Website: www.posta.hu

VII. CHAPTER
SUMMARY OF YOUR RIGHTS

The Data Controller primarily welcomes inquiries at the e-mail address used for this purpose: adatvedelem@hungarianexperience.hu.

22. Summary information on the Data Subject's rights

In this chapter, for the sake of clarity and transparency, we briefly summarize the rights of the data subject, the detailed information on the exercise of which is provided in the next chapter.

Right to prior information
The data subject has the right to receive information about the facts and information related to data management before the start of data management.
(GDPR Article 13-14)
We provide information on the detailed rules in the next chapter.

The data subject's right of access
The data subject has the right to receive feedback from the Data Controller as to whether his personal data is being processed, and if such data processing is underway, he is entitled to access the personal data and related information as defined in the GDPR.
(GDPR Article 15).
We provide information on the detailed rules in the next chapter.

Right to rectification
The data subject is entitled to have the Data Controller correct inaccurate personal data concerning him without undue delay upon request. Taking into account the purpose of the data management, the data subject is entitled to request the completion of incomplete personal data, including by means of a supplementary statement.
(GDPR Article 16).

The right to erasure ("the right to be forgotten")
The data subject has the right to request that the Data Controller delete the personal data concerning him without undue delay, and the Data Controller is obliged to delete the personal

data concerning the data subject without undue delay if one of the reasons specified in the GDPR exists.
(GDPR Article 17)
We provide information on the detailed rules in the next chapter.

The right to restrict data processing
The data subject has the right to request that the Data Controller restricts data processing if the conditions specified in the GDPR are met.
(GDPR Article 18)
We provide information on the detailed rules in the next chapter.

Notification obligation related to the correction or deletion of personal data or the limitation of data management
The Data Controller informs all recipients of all corrections, deletions or data management restrictions to whom or to whom the personal data was disclosed, unless this proves to be impossible or requires a disproportionately large effort. At the request of the data subject, the Data Controller informs about these recipients.
(GDPR Article 19)

The right to data portability
According to the conditions written in the GDPR, the data subject is entitled to receive the personal data concerning him/her provided to the Data Controller in a segmented, widely used, machine-readable format, and is also entitled to forward this data to another Data Controller without this would be hindered by the Data Controller to whom the personal data was made available.
(GDPR Article 20)
We provide information on the detailed rules in the next chapter.

The right to protest
The data subject has the right to object to his personal data at any time for reasons related to his own situation under point e) of Article 6 (1) of the GDPR (the data processing is in the public interest or necessary for the performance of a task carried out in the framework of the exercise of public authority conferred on the Data Controller) or point f) (the data processing is necessary to assert the legitimate interests of the Data Controller or a third party) against its treatment based on this, including profiling based on the aforementioned provisions.
(GDPR Article 21)
We provide information on the detailed rules in the next chapter.

Automated decision-making in individual cases, including profiling
The data subject has the right not to be covered by the scope of a decision based solely on automated data management, including profiling, which would have a legal effect on him or affect him to a similar extent.
(GDPR Article 22)
We provide information on the detailed rules in the next chapter.

Restrictions
The EU or Member State law applicable to the Data Controller or data processor may limit the provisions of Articles 12-22 through legislative measures. Article and Article 34, as well as Articles 12–22. in accordance with the rights and obligations defined in Article 5, the scope of the rights and obligations contained in Article 5, i.e. the enforcement of the basic principles.
(GDPR Article 23)
We provide information on the detailed rules in the next chapter.

Informing the data subject about the data protection incident
If the data protection incident is likely to involve a high risk for the rights and freedoms of natural persons, the Data Controller shall inform the data subject of the data protection incident without undue delay.
(GDPR Article 34)
We provide information on the detailed rules in the next chapter.

The right to lodge a complaint with the supervisory authority (right to an official remedy)

The data subject has the right to file a complaint with a supervisory authority - in particular in the Member State of his or her usual place of residence, workplace or the place of the suspected infringement - if, in the opinion of the data subject, the handling of personal data concerning him/her violates the GDPR.
(GDPR Article 77)
We provide information on the detailed rules in the next chapter.

The right to an effective judicial remedy against the supervisory authority

judicial remedy against the legally binding decision of the supervisory authority concerning them , or if the supervisory authority does not deal with the complaint, or does not inform the person concerned about the procedural developments related to the submitted complaint or its result within three months.
(GDPR Article 78)
We provide information on the detailed rules in the next chapter.

The right to an effective judicial remedy against the controller or processor

All data subjects are entitled to an effective judicial remedy if, in their opinion, their rights under the GDPR have been violated as a result of handling their personal data in accordance with the GDPR.
(GDPR Article 79)
We provide information on the detailed rules in the next chapter.

VIII. CHAPTER
DETAILED INFORMATION ABOUT YOUR RIGHTS

The Data Controller primarily welcomes inquiries at the e-mail address used for this purpose: adatvedelem@hungarianexperience.hu.

23. Right to prior information

The data subject has the right to receive information about the facts and information related to data management before the start of data management

24. Information to be made available if the data is collected from the data subject

24.1. If the personal data concerning the data subject is collected from the data subject, the data controller shall provide the data subject with all of the following information at the time of obtaining the personal data:

a) the identity and contact details of the data controller and, if any, the representative of the data controller;
b) contact details of the data protection officer, if any;
c) the purpose of the planned processing of personal data and the legal basis of data processing;
d) in the case of data management based on point f) of Article 6, paragraph (1) of the GDPR (validation of legitimate interests), the legitimate interests of the data controller or a third party;
e) where applicable, recipients of personal data, or categories of recipients, if any;
f) where applicable, the fact that the data controller wishes to transfer the personal data to a third country or international organization, as well as the existence or absence of a compliance decision by the Commission, or Article 46, Article 47 or Article 49 of the GDPR (1) in the case of data transmission referred to in the second subparagraph of paragraph 1, indicating the appropriate and suitable guarantees, as well as a reference to the methods for obtaining a copy of them or their availability.

24.2. In addition to the information mentioned in point 24.1, the data controller informs the data subject of the following additional information at the time of obtaining the personal data, in order to ensure fair and transparent data management:

a) on the period of storage of personal data, or if this is not possible, on the criteria for determining this period;

b) the data subject's right to request from the data controller access to personal data relating to him, their correction, deletion or restriction of processing, and to object to the processing of such personal data, as well as the data subject's right to data portability;
c) in the case of data processing based on point a) of Article 6 (1) of the GDPR (consent of the data subject) or point a) of Article 9 (2) of the GDPR (consent of the data subject), the right to withdraw consent at any time, which is not affects the legality of data processing carried out on the basis of consent before withdrawal;
d) on the right to submit a complaint to the supervisory authority;
e) whether the provision of personal data is based on legislation or a contractual obligation or is a prerequisite for the conclusion of a contract, as well as whether the data subject is obliged to provide personal data, and what possible consequences the failure to provide data may have;
f) the fact of automated decision-making referred to in paragraphs (1) and (4) of Article 22 of the GDPR, including profiling, as well as, at least in these cases, comprehensible information about the logic used and the significance of such data management and for the data subject what are the expected consequences.

24.3. If the data controller wishes to carry out further data processing of the personal data for a purpose other than the purpose of their collection, it must inform the data subject of this different purpose and of all relevant additional information mentioned in paragraph (2) before the further data processing.

24.4. Points 24.1-3 do not apply if and to what extent the data subject already has the information. (Article 13 GDPR)

25. Information to be made available if the data was not obtained from the data subject

25.1. If the personal data was not obtained from the data subject, the data controller provides the data subject with the following information:

a) the identity and contact details of the data controller and, if any, the representative of the data controller;
b) contact details of the data protection officer, if any;
c) the purpose of the planned processing of personal data and the legal basis of data processing;
d) categories of personal data concerned;
e) recipients of personal data, or categories of recipients, if any;
f) where appropriate, the fact that the data controller wishes to forward the personal data to a recipient in a third country or an international organization, and the existence or absence of a compliance decision by the Commission, or Article 46, Article 47 or Article 49 of the GDPR. in the case of data transmission referred to in the second subparagraph of paragraph (1) of Article 2, the indication of appropriate and suitable guarantees, as well as a reference to the methods for obtaining a copy of them or their availability.

25.2. In addition to the information mentioned in point 25.1, the data controller provides the data subject with the following additional information necessary to ensure fair and transparent data management for the data subject:

a) the period of storage of personal data, or if this is not possible, the criteria for determining this period;
b) if the data management is based on point f) of Article 6 (1) of the GDPR (legitimate interest), on the legitimate interests of the data controller or a third party;
c) the data subject's right to request from the data controller access to personal data relating to him, their correction, deletion or limitation of processing, and to object to the processing of personal data, as well as the data subject's right to data portability;
d) in the case of data processing based on point a) of Article 6 (1) of the GDPR (consent of the data subject) or point a) of Article 9 (2) of the GDPR (consent of the data subject), the right to withdraw consent at any time, which is not affects the legality of data processing carried out on the basis of consent before withdrawal;
e) the right to submit a complaint addressed to a supervisory authority;
f) the source of the personal data and, where appropriate, whether the data comes from publicly available sources; and

g) the fact of automated decision-making referred to in Article 22 (1) and (4) of the GDPR, including profiling, as well as, at least in these cases, comprehensible information about the logic used and the significance of such data management for the data subject what are the expected consequences.

25.3. The data controller provides the information according to points 25.1 and 25.2 as follows:

a) taking into account the specific circumstances of the handling of personal data, within a reasonable time from the acquisition of the personal data, but within one month at the latest;
b) if the personal data is used for the purpose of contacting the data subject, at least during the first contact with the data subject; obsession
c) if it is expected that the data will be communicated to another recipient, at the latest when the personal data is communicated for the first time.

25.4. If the data controller wishes to carry out further data processing of personal data for a purpose other than the purpose for which they were obtained, it must inform the data subject of this different purpose and all relevant additional information mentioned in point 22.2 before further data processing.

25.5. Section 25.1-4 shall not apply if and to the extent that:
a) the data subject already has the information;
b) the provision of the information in question proves to be impossible or would require a disproportionately large effort, especially in the case of data management carried out for the purpose of archiving in the public interest, for scientific and historical research purposes or for statistical purposes, taking into account the conditions and guarantees contained in Article 89 (1) of the GDPR, or if the obligation referred to in paragraph (1) of this article would likely make it impossible or seriously jeopardize the achievement of the goals of this data management. In such cases, the data controller must take appropriate measures - including making the information publicly available - in order to protect the rights, freedoms and legitimate interests of the data subject;
c) the acquisition or disclosure of the data is expressly required by the EU or Member State law applicable to the data controller, which provides for appropriate measures to protect the legitimate interests of the data subject; obsession
d) personal data must remain confidential on the basis of the obligation of professional confidentiality prescribed by an EU or member state law, including the obligation of confidentiality based on legislation.
(Article 14 GDPR)

26. The data subject's right of access

26.1. The data subject is entitled to receive feedback from the Data Controller as to whether his personal data is being processed, and if such data processing is underway, he is entitled to access the personal data and the following information:

a) the purposes of data management;
b) categories of personal data concerned;
c) the recipients or categories of recipients to whom or to whom the personal data has been or will be communicated, including in particular recipients in third countries and international organizations;
d) where appropriate, the planned period of storage of personal data, or if this is not possible, the criteria for determining this period;
e) the right of the data subject to request from the Data Controller the correction, deletion or restriction of processing of personal data concerning him and to object to the processing of such personal data;
f) the right to submit a complaint addressed to a supervisory authority;
g) if the data were not collected from the data subject, all available information about their source;
h) the fact of automated decision-making referred to in paragraphs (1) and (4) of Article 22 of the GDPR, including profiling, as well as, at least in these cases, comprehensible information about the logic used and the significance of such data management and the data subject looking at the expected consequences.

26.2. If personal data is transferred to a third country or an international organization, the data subject is entitled to receive information about the appropriate guarantees in accordance with Article 46 of the GDPR regarding the transfer.

26.3. The Data Controller provides a copy of the personal data that is the subject of data management to the data subject. For additional copies requested by the data subject, the Data Controller may charge a reasonable fee based on administrative costs. If the data subject submitted the request electronically, the information must be provided in a widely used electronic format, unless the data subject requests otherwise. The right to request a copy must not adversely affect the rights and freedoms of others. (Article 15 GDPR)

27. The right to erasure ("the right to be forgotten")

27.1. The data subject has the right to request that the Data Controller delete the personal data concerning him without undue delay, and the Data Controller is obliged to delete the personal data concerning the data subject without undue delay if one of the following reasons exists:

a) the personal data are no longer needed for the purpose for which they were collected or otherwise processed;
b) the data subject withdraws the consent that forms the basis of the data management pursuant to point a) of Article 6 (1) or point a) of Article 9 (2) of the GDPR, and there is no other legal basis for the data management;
c) the data subject objects to the data processing based on Article 21 (1) of the GDPR and there is no overriding legal reason for data processing, or the data subject objects to the data processing based on Article 21 (2);
d) personal data were handled unlawfully;
e) personal data must be deleted in order to fulfill the legal obligation prescribed by EU or member state law applicable to the Data Controller;
f) the collection of personal data took place in connection with the offer of information society-related services referred to in Article 8 (1) of the GDPR.

27.2. If the Data Controller has disclosed the personal data and is obliged to delete it pursuant to point 23.1 above, it will take reasonable steps, including technical measures, taking into account the available technology and the costs of implementation, in order to inform the Data Controllers handling the data that the data subject requested from them the deletion of the links to the personal data in question or the copy or duplicate of this personal data.

27.3. 27.1. and point 27.2 does not apply if data management is necessary:

a) for the purpose of exercising the right to freedom of expression and information;
b) for the purpose of fulfilling the obligation according to EU or member state law applicable to the Data Controller requiring the processing of personal data, or for the execution of a task carried out in the public interest or in the context of the exercise of public authority vested in the Data Controller;
c) on the basis of public interest in the field of public health in accordance with points h) and i) of Article 9 (2) and Article 9 (3) of the GDPR;
d) in accordance with Article 89 (1) of the GDPR for the purpose of archiving in the public interest, for scientific and historical research purposes or for statistical purposes, if the right mentioned in point 1 would likely make this data management impossible or seriously jeopardize it; obsession
e) to present, enforce and defend legal claims.
(GDPR Article 17)

28. The right to restrict data processing

28.1. The data subject has the right to request that the Data Controller restricts data processing if one of the following conditions is met:

a) the data subject disputes the accuracy of the personal data, in which case the limitation applies to the period that allows the Data Controller to check the accuracy of the personal data;
b) the data management is illegal and the data subject opposes the deletion of the data and instead requests the restriction of their use;

c) the Data Controller no longer needs the personal data for the purpose of data management, but the data subject requires them to present, enforce or defend legal claims; obsession
d) the data subject has objected to data processing in accordance with Article 21 (1) of the GDPR; in this case, the restriction applies to the period until it is determined whether the Data Controller's legitimate reasons take precedence over the data subject's legitimate reasons.

28.2. If the data management is subject to restrictions based on point 28.1, such personal data, with the exception of storage, will only be processed with the consent of the data subject, or for the presentation, enforcement or defense of legal claims, or for the protection of the rights of another natural or legal person, or for the purposes of the Union or a member state can be handled in the public interest.

28.3. The Data Controller informs the data subject, at whose request the data management was restricted based on point 28.1, of the lifting of the data management restriction in advance. (GDPR Article 18)

29. The right to data portability

29.1. The data subject has the right to receive the personal data concerning him/her provided to a Data Controller in a segmented, widely used, machine-readable format, and is also entitled to transmit this data to another Data Controller without being hindered by the Data Controller whose provided the personal data if:

a) data management is based on consent pursuant to point a) of Article 6 (1) or point a) of Article 9 (2) of the GDPR, or on a contract pursuant to point b) of Article 6 (1) of the GDPR; and
b) data management takes place in an automated manner.

29.2. When exercising the right to data portability in accordance with point 26.1, the data subject is entitled - if this is technically possible - to request the direct transfer of personal data between Data Controllers.

29.3. The exercise of this right may not violate Article 17 of the GDPR. The aforementioned right does not apply in the event that the data processing is in the public interest or is necessary for the execution of a task performed in the context of the exercise of public authority rights vested in the Data Controller.

29.4. The right mentioned in point 29.1 cannot adversely affect the rights and freedoms of others. (GDPR Article 20)

30. The right to protest

30.1. The data subject has the right to object to his personal data at any time for reasons related to his own situation under point e) of Article 6 (1) of the GDPR (the data processing is in the public interest or necessary for the performance of a task carried out in the framework of the exercise of public authority conferred on the Data Controller) or point f) (the data processing against processing based on the Data Controller or necessary to assert the legitimate interests of a third party), including profiling based on the aforementioned provisions. In this case, the Data Controller may no longer process the personal data, unless the Data Controller proves that the data processing is justified by compelling legitimate reasons that take precedence over the interests, rights and freedoms of the data subject, or that are necessary for the presentation, enforcement or defense of legal claims are connected.

30.2. If personal data is processed for direct business acquisition, the data subject has the right to object at any time to the processing of personal data concerning him for this purpose, including profiling, if it is related to direct business acquisition.

30.3. If the data subject objects to the processing of personal data for the purpose of direct business acquisition, then the personal data may no longer be processed for this purpose.

30.4. The right mentioned in points 30.1 and 30.2 must be specifically brought to the attention of the data subject during the first contact at the latest, and the relevant information must be displayed clearly and separately from all other information.

30.5. In connection with the use of services related to the information society and deviating from Directive 2002/58/EC, the data subject may also exercise the right to object using automated means based on technical specifications.

30.6. If personal data is processed for scientific and historical research or statistical purposes in accordance with Article 89 (1) of the GDPR, the data subject has the right to object to the processing of personal data concerning him for reasons related to his own situation, unless the data management is necessary in order to perform a task carried out for reasons of public interest. (GDPR Article 21)

31. Automated decision-making in individual cases, including profiling

31.1. The data subject has the right not to be covered by the scope of a decision based solely on automated data management, including profiling, which would have a legal effect on him or affect him to a similar extent.

31.2. Clause 31.1 does not apply if the decision:
a) necessary for the conclusion or fulfillment of the contract between the data subject and the Data Controller;
b) it is made possible by EU or member state law applicable to the Data Controller, which also establishes appropriate measures to protect the rights and freedoms and legitimate interests of the data subject; obsession
c) is based on the express consent of the data subject.

31.3. In the cases referred to in points a) and c) of point 31.2, the Data Controller is obliged to take appropriate measures to protect the rights, freedoms and legitimate interests of the data subject, including at least the right of the data subject to request human intervention on the part of the Data Controller, to express his point of view, and with the decision file an objection against.

31.4. 31.2. the decisions referred to in point 1 may not be based on the special categories of personal data referred to in Article 9(1) of the GDPR, unless points a) or g) of Article 9(2) apply and the protection of the data subject's rights, freedoms and legitimate interests appropriate measures were taken. (GDPR Article 22)

32. Restrictions

32.1. The EU or Member State law applicable to the Data Controller or data processor may limit the provisions of Articles 12-22 of the GDPR through legislative measures. Article and Article 34, as well as Articles 23–31. with regard to its provisions in accordance with the rights and obligations set out in Article 5, the scope of the rights and obligations contained in Article 5, if the restriction respects the essential content of fundamental rights and freedoms, as well as a necessary and proportionate measure for the protection of the following in a democratic society:

a) national security;
b) national defense;
c) public safety;
d) prevention, investigation, detection or prosecution of crimes, as well as the implementation of criminal sanctions, including protection against threats to public safety and the prevention of these threats;
e) other important general public interest objectives of the Union or a Member State, in particular an important economic or financial interest of the Union or a Member State, including monetary, budgetary and tax issues, public health and social security;
f) protection of judicial independence and judicial proceedings;
g) in the case of regulated occupations, the prevention, investigation and detection of ethical violations and the conduct of related procedures;
h) in the cases mentioned in points a) -e) and ag) - even occasionally - control, investigation or regulatory activities related to the performance of public authority tasks;
i) the protection of the data subject or the protection of the rights and freedoms of others;
j) enforcement of civil law claims.

32.2. The legislative measures referred to in point 32.1 contain, where appropriate, detailed provisions at least:

a) for the purposes of data management or the categories of data management,
b) categories of personal data,
c) the scope of the restrictions introduced,
d) guarantees aimed at preventing misuse, unauthorized access or transmission,
e) to define the Data Controller or to define the categories of Data Controllers,
f) for the duration of data storage, as well as applicable guarantees, taking into account the nature, scope and purposes of data management or data management categories,
g) risks affecting the rights and freedoms of the data subjects, and
h) the right of the data subjects to receive information about the restriction, unless this may adversely affect the purpose of the restriction.
(GDPR Article 23)

33. Informing the data subject about the data protection incident

33.1. If the data protection incident is likely to involve a high risk for the rights and freedoms of natural persons, the Data Controller shall inform the data subject of the data protection incident without undue delay.

33.2. the information and measures mentioned in points b), c) and d) of Article 33, paragraph (3) of the GDPR must be communicated.

33.3. The data subject does not need to be informed as mentioned in point 33.1 if any of the following conditions are met:
a) the Data Controller has implemented appropriate technical and organizational protection measures, and these measures have been applied to the data affected by the data protection incident, in particular those measures - such as the use of encryption - that would be incomprehensible to persons not authorized to access personal data they make the data;
b) after the data protection incident, the Data Controller has taken additional measures to ensure that the high risk to the rights and freedoms of the data subject referred to in point 1 is unlikely to materialize in the future;
c) providing information would require a disproportionate effort. In such cases, the data subjects must be informed through publicly published information, or a similar measure must be taken that ensures similarly effective information to the data subjects.

33.4. If the Data Controller has not yet notified the data subject of the data protection incident, the supervisory authority, after considering whether the data protection incident is likely to involve a high risk, may order the data subject to be informed or establish that one of the conditions mentioned in point 3 has been met. (GDPR Article 34)

34. The right to complain to the supervisory authority

34.1. Without prejudice to other administrative or judicial remedies, all data subjects have the right to file a complaint with a supervisory authority (National Data Protection Authority) - in particular in the Member State of their usual place of residence, workplace or the place of the alleged infringement - if, in the judgment of the data subject, the the processing of relevant personal data violates this GDPR.

34.2. The supervisory authority to which the complaint was submitted is obliged to inform the customer about the procedural developments related to the complaint and its outcome, including that the customer is entitled to judicial redress based on Article 78 of the GDPR. (GDPR Article 77)

34.3. The contact details of the National Data Protection Authority are as follows:

Address: 1055 Budapest, Falk Miksa utca 9-11.
Mailing address: 1363 Budapest, Pf.: 9.
Website: www.naih.hu
Phone: +36 (30) 683-5969; +36 (30) 549-6838; +36 (1) 391 1400
Fax: +36 (1) 391-1410
E-mail: ugyfelszolgalat@naih.hu

35. The right to an effective judicial remedy against the supervisory authority

35.1. Without prejudice to other administrative or non-judicial remedies, all natural and legal persons are entitled to an effective judicial remedy against the legally binding decision of the supervisory authority .

35.2. Without prejudice to other administrative or non-judicial legal remedies, all data subjects are entitled to an effective judicial remedy if the competent supervisory authority based on Article 55 or 56 of the GDPR does not deal with the complaint or does not inform the data subject within three months in accordance with Article 77 about procedural developments or the result of a complaint filed under

35.3. Proceedings against the supervisory authority must be initiated before the court of the Member State where the supervisory authority is based.

35.4. If proceedings are initiated against a decision of the supervisory authority in relation to which the Board previously issued an opinion or made a decision within the framework of the uniformity mechanism, the supervisory authority is obliged to send this opinion or decision to the court. (GDPR Article 78)

36. The right to a judicial remedy against the controller or data processor

36.1. Without prejudice to the available administrative or non-judicial legal remedies, including the right to complain to the supervisory authority according to Article 77 of the GDPR, all data subjects are entitled to an effective judicial remedy if, in their judgment, their personal data has been improperly handled in accordance with this GDPR your rights under this GDPR have been violated.

36.2. Proceedings against the data controller or data processor must be initiated before the court of the Member State where the data controller or data processor operates. Such a procedure can also be initiated before the court of the Member State of the habitual residence of the person concerned, unless the data controller or the data processor is a public authority of a Member State acting in the capacity of public authority. (GDPR Article 79)

IX. CHAPTER
SUBMISSION OF THE APPLICANT'S REQUEST, MEASURES OF THE DATA PROCESSOR

37. Submitting a request, actions of the Data Controller

37.1. **The Data Controller primarily welcomes inquiries at the e-mail address used for this purpose: adatvedelem@hungarianexperience.hu .** The Data Controller shall inform the data subject without undue delay, but in any case within one month of the receipt of the request, of the measures taken as a result of his request to exercise his rights.

37.2. If necessary, taking into account the complexity of the application and the number of applications, this deadline can be extended by another two months. The Data Controller shall inform the data subject of the extension of the deadline, indicating the reasons for the delay, within one month of receiving the request.

37.3. If the data subject submitted the request electronically, the information must be provided electronically, if possible, unless the data subject requests otherwise.

37.4. If the Data Controller does not take measures following the data subject's request, it shall inform the data subject without delay, but at the latest within one month of the receipt of the request, of the reasons for the failure to take action, and of the fact that the data subject may file a complaint with a supervisory authority and exercise his right to judicial redress.

37.5. The Data Controller provides information in accordance with Articles 13 and 14 of the GDPR and information about the rights of the data subject (Articles 15-22 and 34 of the Regulation) and measures free of charge. If the data subject's request is clearly unfounded or - especially due to its repeated nature - excessive, the Data Controller, taking into account the

administrative costs associated with providing the requested information or information or taking the requested measure:
a) may charge a fee, or
b) may refuse to take action based on the request.
It is the responsibility of the Data Controller to prove that the request is clearly unfounded or exaggerated.

37.6. If the Data Controller has reasonable doubts about the identity of the natural person who submitted the request, it may request the provision of additional information necessary to confirm the identity of the person concerned.