PRIVACY NOTICE

1. The Data Controller (Service Provider)

Name of the service provider: Safari Park Kft.
Head office and postal address: 2750 Nagykőrös, Szurdok dűlő 812.
Registration authority: Budapest-Capital Regional Court as the Company Registry Court
Company registration number: Cg. 01-06-734244
VAT identification number: 20720494-2-42
E-mail: info@safaripark.hu
Website: www.safaripark.hu
Customer service phone number: +36 30 905 5201
Customer service email: info@safaripark.hu
Complaints handling place and contact details: 1145 Budapest, Thököly út 111., +36 30 905 5201, info@safaripark.hu (On working days between 10.00 and 16.00.)
Name of hosting service provider: Webter-Media Kft.
Address of hosting service provider: 3020 Petőfibánya, Hegyalja utca 35.

I. Privacy Policy Applied by the Company

1. As the data controller, the Service Provider undertakes to ensure that all data processing in relation to its activities complies with the requirements set out in this Policy and the applicable legislation.

2. Information about the Service Provider's data management is constantly available in the footer of the home page of the website www.safaripark.hu .

3. The Service Provider is entitled to unilaterally amend the Privacy Policy. If the Privacy Policy is amended, the Service Provider shall notify the User by publishing the changes on www.safaripark.hu at least eight (8) days before the amendment comes into force. By using the Service after the effective date of the amendment, the User accepts the amended Privacy Policy.

4. The Service Provider is committed to the protection of the User's personal data and considers it of utmost importance to respect their right to informational self-determination. The Service Provider handles personal data confidentially and implements all security, technical, and organisational measures to guarantee the security of the data.

The Service Provider's data management principles are in compliance with the applicable legislation on data protection, in particular with the following:

Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (hereinafter the Avtv., Data Protection Act);

Act CVIII of 2001 on Electronic Commerce and on Information Society Services (Eker. tv.);

Act XLVIII of 2008 on Essential Conditions of and Certain Limitations to Business Advertising activity.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

The Service Provider will use the personal data necessary for the provision of its services on the basis of the consent of the data subjects and only for the purposes for which they are intended.

The Company undertakes to provide clear, attention-grabbing, and unambiguous communication to Users before the collection, recording, or processing of any Personal Data, informing them of the method, purpose, and principles of data collection. In addition, in all cases where the collection, processing, or recording of data is not required by law, the Company calls the User's attention to the voluntary nature of the data provision. In the case of mandatory data provision, the legal act imposing the processing must also be indicated. The data subject must be informed about the purposes of the processing and the parties that will handle and process the Personal Data.

In all cases where the Company intends to use the Personal Data provided for purposes other than those for which they were originally collected, the Company shall inform the User thereof and obtain their prior explicit consent or provide them with the opportunity to prohibit such use.

When collecting, recording, and processing data, the Service Provider shall in any case comply with the restrictions laid down by law and shall inform the data subject of its activities by electronic mail, as requested. The Company undertakes not to impose any sanctions on any User who refuses to provide the optional data.

II. Legal Basis for Data Processing

1. Personal data may be processed if the data subject consents to it or if it is ordered by law or by a local authority based on authorisation conferred by law concerning specific data defined therein for the performance of a task carried out in the public interest. The legal basis for data processing is the voluntary consent of the data subject pursuant to Section 5 (1) a) of Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (Avtv.) and Section 13/A of Act CVIII of 2001 on Electronic Commerce and on Information Society Services.
2. The consent of a legal representative is required for the declaration of an incapacitated minor or a minor with limited capacity, except for those parts of the service where the declaration is for the purpose of registration that occurs in the mass of everyday life and does not require special consideration. The consent or subsequent approval of the legal representative of a minor aged 16 or over is not required for the validity of the declaration of consent of the data subject.
3. Where the personal data have been collected with the consent of the data subject, the data controller may, unless otherwise provided by law, process the personal data collected without further specific consent and even after the withdrawal of the data subject's consent
4. a) for the purposes of complying with a legal obligation, or
5. b) for the purposes of the legitimate interest pursued by the controller or by a third party, where such interest is proportionate to the restriction of the right to the protection of personal data.

1. Purpose of the Processing and Scope of the Data Processed, Duration of the Processing, Persons Entitled To Access the Data

Personal data may only be processed for specified purposes, for the exercise of rights and the performance of obligations. At all stages of processing, the purpose of the processing must be fulfilled and the collection and processing of data must be fair and lawful. Only personal data that is necessary to achieve the purpose of the processing and is suitable for achieving that purpose may be processed. Personal data may only be processed to the extent and for the duration necessary to achieve the purpose. The data processing of the Service Provider's services is based on voluntary consent, however, in certain cases, the processing, storage, and transmission of some of the data provided is required by law. The Service Provider will not use the personal data for purposes other than those stated.

2. Booking an appointment to visit the Safari Park

The processing is based on the User's voluntary, duly informed declaration, which, in the case of booking an appointment, is necessary to use the booking service on the website. The declaration contains the express consent of the Users to the processing of their personal data provided during the use of the site. The legal basis for data processing is the voluntary consent of the data subject pursuant to Section 5 (1) a) of Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information and Section 169(2) of Act C of 2000 on Accounting.

The purpose of the data processing is to ensure the provision of the booking service on the website, the booking and its servicing, and the documentation of the visit. Furthermore, the purpose of data processing is to identify the User as a reserving user, as well as to perform the reserved service, to send notifications related to it, to register the Users and to distinguish them from each other. Data processed: first and last name, telephone number, e-mail, car registration number. Duration of data processing: 8 years

3. Webpages of the Service Provider

The HTML code of the portal contains links from and to external servers independent of Nemzetközi Cirkusz Bt. The providers of these links are able to collect User Data due to the direct connection to their servers.

An external service provider helps to independently measure website traffic and other web analytics data (Google Analytics). The data controller can provide detailed information on the processing of measurement data; contact details: http://www.google.com/analytics.

4. Cookie

The Company places small data packets (so-called "cookies") on the User's computer in order to provide a personalised service. The purpose of the cookies is to ensure the highest possible quality of the operation of the site in order to enhance the User's experience. By visiting the website and using some of its functions, you consent to the storage of these cookies on your computer and their access by the Data Controller. Unless otherwise specified, cookies are stored for 30 days. However, users have the option to configure and block cookie-related activities through their web browser settings. The risk of a User provision other than the default setting is that without the use of cookies, you may not be able to use all the services of the website.

5. Statistical data

The Service Provider may use the data for statistical purposes. The use of data in aggregate statistical form shall not include the name or any other identifiable data of the User concerned.

6. Data to be technically recorded during the operation of the system

The data that are technically recorded during the operation of the system are the data of the User's computer that is generated during the use of the service and recorded by the data controller's system as an automatic result of technical processes. The data that is automatically recorded is automatically logged by the system at login and logout without any special declaration or action by the User. This data may not be linked to other personal data of users, except where required by law. Only the Data Controller has access to the data. The purpose of the automatically collected data is to ensure the provision of the services available through the Company's web pages, the display of personalised content and advertisements, the production of statistics, the technical development of the IT system, the protection of Users' rights and the analysis of user habits. The Data Controller may use the data made available by Users when using the Service to form User Groups and to display targeted content and/or advertisements on the Company's websites to the User Groups.

Data that are automatically and technically recorded during the operation of the system are stored in the system from the moment they are generated for a period of time that is reasonable to ensure the operation of the system. The Company ensures that these automatically recorded data cannot be linked to other personal data of the user, except in cases required by law. If the User has withdrawn their consent to the processing of their personal data or has unsubscribed from the service, their identity will not be identifiable from the technical data thereafter.

7. Other data processing

The User will be informed of any data processing not listed in this notice when the data is collected. The court, the public prosecutor's office, the investigating authority, the offence authority, the administrative authority, the data protection commissioner or other bodies authorised by law may contact the Data Controller for information, disclosure, transfer of data or provision of documents. The Service Provider shall disclose personal data to the above bodies and authorities only to the extent strictly necessary for the purpose of the request, provided that the authority has indicated the exact purpose and scope of the data.

1. The Data Controller does not verify the Personal Data provided to it. The person providing the information is solely responsible for its correctness. When providing an e-mail address, each User also assumes responsibility for the fact that the e-mail address provided is used exclusively by them. With regard to this assumption of liability, any liability in connection with access to a given e-mail address rests solely with the User who registered the e-mail address. If the User does not provide their own personal data, they are obliged to obtain the consent of the data subject.
2. Personal data may be accessed by employees who have an employment or agency contract with the Service Provider, as well as by courier service employees involved in the delivery of products.

III. Data Transmission

1. The Service Provider shall transfer personal data to third parties – in addition to the provisions of this privacy policy – with the prior and express consent of the User. This provision does not apply to mandatory data transfers based on legislation.
2. The User acknowledges that the following personal data stored by the data controller Safari Park Kft. (2750 Nagykőrös, Szurdok dűlő 812) in the user database of www.safaripark.hu will be transferred to the data processor OTP Mobil Kft. The scope of the data transmitted by the data controller is as follows: e-mail address. The nature and purpose of the data processing activities carried out by the data processor can be found in the SimplePay Privacy Notice, at the following link: http://simplepay.hu/vasarlo-aff.
3. By using the service, the User agrees that the Service Provider may transmit the data to the organiser of the event in question in order to enable the organiser of the event to inform the User directly and immediately about the cancellation of the event, changes to the date of the event, or important circumstances affecting the spectator in any respect, or to directly arrange the refund or exchange of tickets.
4. The Company, as Data Controller, is entitled and obliged to transmit to the competent authorities any personal data at its disposal and stored by it in accordance with the law, which it is obliged to transmit by law or by a final court or official decision. The Controller cannot be held liable for such transfers and the consequences thereof.
5. Where the Service Provider transfers the operation or use of the content service on www.safaripark.hu to a third party, in whole or in part, the Personal Data processed by the Service Provider may be transferred to such third party for further processing without any further consent being required. This transfer of data may only serve to ensure the continuity of the registration of already registered Users, but may not place the User in a more disadvantageous position than the data management and data security rules indicated in the current version of this Privacy Policy

1. Name of the Data Processor

The Service Provider processes the data itself and does not forward them for processing. The delivery of the items will be carried out by the organisation indicated in the confirmation of purchase.

VII. Data Security Measures

1. In connection with the processing and storage of personal data, the Service Provider shall exercise the utmost care. In the area of IT security, the Service Provider shall use the most effective, state-of-the-art tools and procedures reasonably available.
2. The Controller shall design and implement the data processing operations in such a way as to ensure the protection of the privacy of the data subjects.
3. Controllers, and within their sphere of competence, data processors must implement adequate safeguards and appropriate technical and organisational measures to protect personal data, as well as adequate procedural rules to enforce the provisions of the Avtv. and other regulations concerning confidentiality and security of data processing.
4. In particular, appropriate measures shall be taken to protect the data against unauthorised access, alteration, transmission, public disclosure, deletion or destruction, accidental destruction or accidental damage and against inaccessibility resulting from changes in the technology used.
5. For the protection of data sets stored in different electronic filing systems, suitable technical solutions shall be introduced to prevent – unless this is permitted by law – the interconnection of data stored in these filing systems and the identification of the data subjects.
6. In respect of automated personal data processing, data controllers and processors shall implement additional measures designed toa jogosulatlan adatbevitel megakadályozását;
   - **a.** prevent the unauthorised entry of data;
   - **b.** prevent the use of automated data-processing systems by unauthorised persons using data transfer devices;
   - **c.** ensure that it is possible to verify and establish to which bodies personal data have been or may be transmitted using data transfer devices;
   - **d.** ensure that it is possible to verify and establish which personal data have been entered into automated data-processing systems and when and by whom the data were input;
   - **e.** ensure that installed systems may, in case of malfunctions, be restored; and
   - **f.** that errors in automated processing are reported.

7. The controller and the processor should take into account the state of the art when defining and implementing data security measures. Where alternate data processing solutions are available, the one selected shall ensure the highest level of protection of personal data, except if this would entail unreasonable hardship for the data controller.
8. The Service Provider selects and operates the IT tools used to process personal data in the course of providing the service in such a way that the processed data is

- **a.** accessible to authorised persons (availability);
- **b.** its authenticity and verification are secured (authenticity of processing);
- **c.** the integrity of the data can be verified (data integrity);
- **d.** it is protected against unauthorised access (data confidentiality)

9. The Service Provider shall ensure the security of data processing by technical, organisational, and structural measures that provide a level of protection appropriate to the risks associated with data processing.
10. In the course of data processing, the Service Provider shall retain

- **a.** confidentiality: it protects the information so that only authorised persons have access to it;
- **b.** integrity: protects the accuracy and completeness of the information and the method of processing;
- **c.** availability: ensuring that the rightful user has effective access to the information he needs and the means to access it when he needs it.

11. The Service Provider's IT system and network are protected against computer fraud, espionage, sabotage, vandalism, fire and flood, computer viruses, computer hacking and denial of service attacks. The Service Provider ensures security through server-level and application-level security procedures.
12. Electronic messages transmitted over the Internet, regardless of the protocol (e-mail, web, FTP etc.), are vulnerable to network threats that could lead to fraudulent activity or to the disclosure or modification of information. The Service Provider will take all reasonable precautions to prevent such threats. It monitors systems in order to record and provide evidence of any security incidents. However, the Internet is not 100% secure, as is well-known and understood by Users. The Service Provider shall not be liable for any damage caused by indefensible attacks that occur despite the exercise of reasonable care.

VIII. Rights of Data Subjects and Their Enforcement, Objection to Processing of Personal Data, Judicial Enforcement of Rights and Compensation

1. A change in personal data or a request for the deletion of personal data may be communicated by means of a written statement in a private document with full probative value sent from the registered e-mail address or by post. In addition, some Personal Data may be changed by making changes to the personal profile page. Once a request for the deletion or modification of personal data has been fulfilled, the previous (deleted) data can no longer be restored.

Users may request information about the processing of their personal data. A request for information sent by e-mail is considered authentic by the Data Controller only if it is sent from the registered e-mail address of the User. At the request of the data subject, the Controller shall provide information about the data of the data subject processed by the controller or by a processor on its behalf, the source of the data, the purpose, legal basis, and duration of the processing, the name and address of the processor and the activities related to the processing, and, in the case of transfer of personal data of the data subject, the legal basis and the recipient of the transfer. The request for information shall be sent by e-mail to info@safaripark.hu. The Service Provider shall provide the information in writing in an intelligible form within the shortest possible time from the date of the request, but not later than 30 days, upon the request of the data subject.

The information under this point shall be provided free of charge if the person requesting the information has not yet submitted a request for information to the controller for the same set of data in the current year. In other cases, compensation may be granted. Reimbursement of costs already paid will be required if the data have been unlawfully processed or if the request for information has led to a correction.

The data controller may refuse to provide the data subject with information only in the cases specified in the Avtv. In case of refusal to provide information, the controller shall inform the data subject in writing of the provision of this Act on the basis of which the information was refused. In the case of refusal to disclose, the data controller shall inform the data subject of the possibility of judicial remedy and recourse to the National Authority for Data Protection and Freedom of Information (hereinafter referred to as "the Authority"). The controller shall notify the Authority of rejected applications annually by 31 January of the year following the year in question.

2. The data subject may request the controller to rectify his or her personal data and to erase or block his or her personal data, except for mandatory processing.
3. For the purposes of monitoring the lawfulness of the transfer and informing the data subject, the controller shall keep a record of the transfer, which shall include the date of the transfer of personal data processed by the controller, the legal basis and the recipient of the transfer, the scope of the personal data transferred and other data specified in the legislation providing for the processing.

4. If the personal data is not accurate and the accurate personal data is available to the controller, the controller shall correct the personal data.

5. The personal data must be deleted if

- **a.** the processing is unlawful;
- **b.** the data subject requests it, as provided for in the Avtv;
- **c.** it is incomplete or incorrect, a situation which cannot be lawfully remedied, provided that cancellation is not precluded by law;
- **d.** the purpose of the processing has ceased to exist or the statutory time limit for the storage of the data has expired;
- **e.** ordered by a court or the Authority

6. In the case referred to in point (d) of the above paragraph, the obligation to delete shall not apply to personal data whose data medium is subject to archival custody pursuant to the legislation on the protection of archival material.

7. Instead of deletion, the controller shall block the personal data if the data subject so requests or if, on the basis of the information available to him or her, it is likely that deletion would harm the data subject's legitimate interests. Personal data blocked in this way may be processed only for as long as the processing purpose that precluded the deletion of the personal data persists.
8. The controller shall tag the personal data it processes where the data subject contests the accuracy or correctness of the personal data, but the inaccuracy or incorrectness of the contested personal data cannot be clearly established.
9. The data subject and all those to whom the data were previously disclosed for processing must be informed of the rectification, blocking, tagging and deletion. Notification may be omitted if this does not harm the legitimate interests of the data subject having regard to the purposes of the processing.
10. If the controller does not comply with the data subject's request for rectification, blocking, or deletion, the controller shall, within 30 days of receipt of the request, provide in writing the factual and legal grounds for refusing the request for rectification, blocking, or deletion. If the request for rectification, deletion, or blocking is refused, the controller shall inform the data subject of the possibility of judicial remedy and of recourse to the Authority.
11. The data subject must be informed before the processing starts whether the processing is based on consent or whether it is mandatory.
12. The data subject must be informed clearly and in detail of all facts relating to the processing of his or her data before the processing begins, in particular the purpose and legal basis of the processing, the person authorised to process and control the data, the duration of the processing, if the controller processes the personal data of the data subject pursuant to Section 6 (5) of the Data Protection Act, and who may access the data. The information shall also cover the rights and remedies of the data subject in relation to the processing. In the case of mandatory data processing, the information may also be provided by publishing a reference to the legal provisions containing the information referred to in the above paragraph.

13. The data subject may object to the processing of his or her personal data,

- **a.** where the processing or transfer of personal data is necessary solely for compliance with a legal obligation to which the controller is subject or for the purposes of the legitimate interests pursued by the controller, the recipient or a third party, except in cases of mandatory processing;
- **b.** where the personal data are used or disclosed for the purposes of direct marketing, public opinion polling, or scientific research; and
- **c.** in other cases prescribed by law.

14. The controller shall examine the objection within the shortest possible time from the date of the request, but not later than 15 days, decide whether the objection is justified and inform the applicant in writing of its decision.

15. If the controller establishes that the data subject's objection is justified, the controller shall cease the processing, including further collection and further transfer of data, and block the data; furthermore, the controller shall inform all those to whom the personal data subject to objection has previously been transmitted, and who is obligated to take action to enforce the right to object, about the objection and the measures taken based on it.

If the data subject does not agree with the decision of the controller or if the controller fails to comply with the time limit, the data subject may – within 30 days of the notification of the decision or the last day of the time limit – take the matter to court in the manner provided for in Section 22 of the Avtv.

If the data recipient does not receive the data necessary to exercise his or her rights because of the data subject's objection, he or she may, within 15 days of the notification, take legal action against the controller in order to obtain access to the data, as provided for in Section 22 of the Data Protection Act. The controller may also bring a claim against the data subject.

If the controller fails to give notice, the recipient may request clarification from the controller of the circumstances surrounding the failure to disclose the data, which the controller shall provide within 8 days of the receipt of the recipient's request for such clarification. In case of a request for clarification, the data recipient may turn to the court against the data controller within 15 days from the clarification's provision or, at the latest, from the deadline for providing it. The controller may also bring a claim against the data subject.

The controller may not delete the data subject's data if the processing is required by law. However, the data may not be transferred to the recipient if the controller has consented to the objection or if the court has ruled that the objection is justified.

16. In the event of a breach of the data subject's rights, as well as in the cases provided for in Section 21 of the Data Protection Act, the data subject may take legal action against the controller. The court shall proceed with the case out of turn.

The controller must prove that the processing is in compliance with the law. In cases falling under Subsections (5) and (6) of Section 21 of the Avtv., the lawfulness of data transmission to the recipient shall be proven by the data recipient.

The tribunal has jurisdiction to hear the case. The lawsuit – at the choice of the data subject – may also be initiated before the court of the data subject's domicile or residence.

In the lawsuit, a party may also be someone who otherwise lacks the legal capacity to sue. In the lawsuit, the Data Protection Authority may intervene for the purpose of safeguarding the data subject's interests.

If the court grants the application, the data controller shall be obliged to provide the information, rectify, block or delete the data, annul the decision taken by automated data processing, take into account the right of objection of the data subject, or release the data requested by the data recipient as defined in Section 21 of the Avtv.

If the court rejects the data recipient's application in the cases specified in Section 21 of the Data Protection Act, the data controller is obliged to delete the data subject's personal data within 3 days of the notification of the judgment. The data controller is obliged to delete the data even if the data recipient does not turn to the court within the deadline specified in Subsections (5) and (6) of Section 21 of the Avtv.

The court may order the publication of its judgment, with the publication of the data controller's identification data, if the interests of data protection and the rights of a larger number of data subjects protected by this Act so require.

17. The controller must compensate for the damage caused to others by unlawful processing of the data subject's data or by breaches of data security requirements. The controller is also liable to the data subject for any damage caused by the processor. The controller shall be exempt from liability if it proves that the damage was caused by an unavoidable cause outside the scope of the processing. No compensation shall be paid to the extent that the damage arises from intentional or grossly negligent conduct of the affected party.

IX. Legal options

Further data processing service information at info@safaripark.hu. The User may exercise his or her enforcement rights before the courts under the Data Protection Act and the Civil Code. You can lodge a complaint with the National Authority for Data Protection and Freedom of Information:

Name: National Authority for Data Protection and Freedom of Information mailing address: 1530 Budapest, Post office box: 5. address: 1125 Budapest Szilágyi Erzsébet fasor 22/c

Phone: +36 (1) 391-1400
Fax: +36 (1) 391-1410
E-mail: ugyfelszolgalat@naih.hu URL http://naih.hu

Annexe

Definition of Terms Used in This Privacy Notice

data set: all data processed in a single file;

data controller: a natural or legal person, or organisation without legal personality which, alone or jointly with others, determines the purposes and means of the processing of data; makes and executes decisions concerning data processing (including the means used) or has it executed by a data processor; controller:

1. Nemzetközi Cirkusz Bt. (located at: 1145 Budapest, Thököly út 111.);
2. during each show or event, the Event Organiser for whose event the User has purchased the tickets; the name and details of the Event Organiser can be found on the event data sheet on the magyarnemzeticirkusz website and on the ticket.

data processing: any operation or the totality of operations performed on the data, irrespective of the procedure applied; in particular, collecting, recording, registering, classifying, storing, modifying, using, querying, transferring, disclosing, synchronising or connecting, blocking, deleting and destructing the data, as well as preventing their further use;

data process: performing technical tasks in connection with data processing operations, irrespective of the method and means used for executing the operations, as well as the place of execution, provided that the technical task is performed on the data;

data processor: any natural or legal person or organisation without legal personality processing the data on the grounds of a contract, including contracts concluded pursuant to legislative provisions;

tagging data: marking data with a special ID tag to differentiate it;

data destruction: complete physical destruction of the data carrier recording the data;

data transfer: ensuring access to the data for a specified third party;

data deletion: making data unrecognisable in a way that it can never again be restored;

blocking of data: marking data with a special ID tag to indefinitely or definitely restrict its further processing;

automated dataset: a set of data to be processed automatically;

EEA Member State: any Member State of the European Union and any State which is party to the Agreement on the European Economic Area, as well as any State the nationals of which enjoy the same legal status as nationals of States which are parties to the Agreement on the European Economic Area, based on an international treaty concluded between the European Union and its Member States and a State which is not party to the Agreement on the European Economic Area;

data subject: any natural person directly or indirectly identifiable by reference to specific personal data;

user: a natural person who registers on the Service Provider's website or makes a purchase without registration;

machine processing: includes the following operations when they are carried out wholly or partly by automated means: storage of data, logical or arithmetical operations on data, alteration, deletion, retrieval and dissemination of data;

third country: any state that is not an EEA state;

third party: any natural or legal person, or organisation without legal personality other than the data subject, the data controller or the data processor;

consent: any freely and expressly given specific and informed indication of the will of the data subject by which he signifies his agreement to personal data relating to him being processed fully or to the extent of specific operations;

disclosure: ensuring open access to the data;

personal data: data relating to the data subject, in particular by reference to the name and identification number of the data subject or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity as well as conclusions drawn from the data in regard to the data subject;

objection: a declaration made by the data subject objecting to the processing of their personal data and requesting the termination of data processing, as well as the deletion of the data processed