I. The Data Controller

1. The data processing tasks in this Data Protection Information, in the roles detailed in point I.2., are carried out by the following organizations (hereinafter collectively referred to as: Service Provider):

I/A.

Name:	**European Aquatics**
Registered office:	
Registration authority:	
Registration number:	
Tax nr:	
Represented by:	
Data Protection Officer name:	
Data Protection Officer phone nr:	
Data Protection Officer email:	

I/B. Technical Provider of the application

Name:	InterTicket Kft.
Registered office:	1139 Budapest, Váci út 99.
Registration authority:	Metropolitan Court as Court of Registration
Registration number:	Cg. 01-09-736766
Tax nr:	10384709-2-41
E-mail address:	interticket@interticket.hu
Webpage:	www.jegy.hu
Customer service contact:	Through the chat application, which is availablehere.
Customer service email:	interticket@interticket.hu
Complaint handling location and contact:	1139 Budapest, Váci út 99. 6. emelet Through the chat application, which is availablehere. interticket@interticket.hu Workdays between 10.00 - 16.00
Hosting provider name:	T-Systems Adatpark
Hosting provider address:	1087 Budapest, Asztalos Sándor u. 13.
Data Protection Registration ID:	NAIH-54216/2012.
Data Protection Officer email:	adatvedelmi.tisztviselo@interticket.hu

II. Privacy Policy Applied by the Service Provider

The Service Provider, as the data controller, undertakes to ensure that all data processing related to its activities complies with the expectations defined in this policy, in the applicable national legislation, and in the legal acts of the European Union.

The Service Provider operates the "card system" (hereinafter, for the purposes of this document: City Card application or application). The City Card application utilizes the possibilities offered by the smart card system and mobile application environment, creating an integrated tool with the city card, related services, and the application that creates its virtual environment. This tool serves local economic development, strengthens the identity consciousness of city residents, encourages their activity, and strengthens community decision-making. The City Card application was primarily developed for the citizens of the district, but based on the Municipality's decision, it can also be used by those who work, study, or are otherwise closely connected to the life of the district (hereinafter referred to as: Users).

Information related to the data processing of the Service Provider is continuously available in the City Card application.

The Service Provider is entitled to unilaterally modify this Data Processing Information. In case of modification, the Service Provider will notify the User of the changes by publishing them in the City Card application. The User accepts the modified Data Processing Information by using the service after the modification becomes effective.

The Service Provider is committed to protecting the personal data of its customers and partners and considers it of utmost importance to respect the information self-determination rights of its customers. The Service Provider treats personal data confidentially and takes all security, technical, and organizational measures necessary to guarantee data security. The Service Provider's data processing practice is contained in this Data Processing Information.

The Service Provider's data processing principles align with the applicable data protection laws, in particular:

- Act CXII of 2011 - on the Right to Informational Self-Determination and Freedom of Information (Infotv.);
- Regulation (EU) 2016/679 of the European Parliament and of the Council (April 27, 2016) – on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR);
- Act V of 2013 – on the Civil Code (Ptk.);
- Act C of 2000 – on Accounting (Számv. tv.);
- Act CXXXVI of 2007 – on the Prevention and Combating of Money Laundering and Terrorist Financing (Pmt.);
- Act CVIII of 2001 - on Electronic Commerce Services, and on Certain Issues of Information Society Services (Eker. tv.);
- Act XLVIII of 2008 - on the Basic Requirements and Certain Restrictions of Commercial Advertising Activities (Grt.).

The Service Provider uses personal data based on legal grounds provided by the GDPR and only for specific purposes.

The Service Provider undertakes to provide clear, prominent, and explicit communication before recording or processing any of the User's Personal Data, informing them of the method, purpose, and principles of data collection. In the case of mandatory data provision, the legal regulation ordering the Data Processing must also be specified. The data subject must be informed of the purpose of the Data Processing and of who will process or handle the Personal Data.

In all cases where the Company intends to use the provided Personal Data for a purpose different from the original purpose of data collection, it informs the User and obtains their prior, explicit consent or provides an opportunity for the User to prohibit the use.

III. Legal Basis, Purpose, and Scope of Data Processing, Duration of Data Processing, and Those Entitled to Access Personal Data

1. The Service Provider’s data processing is based on the following legal grounds (GDPR Article 6 (1)):

a) the data subject has given consent for one or more specific purposes (voluntary consent);

b) the data processing is necessary for the performance of a contract to which the data subject is a party or to take steps at the request of the data subject prior to entering into a contract (contract

performance);

c) the data processing is necessary for compliance with a legal obligation to which the controller is subject (legal obligation);

d) the data processing is necessary for the purposes of the legitimate interests pursued by the controller or a third party (legitimate interest).

In the case of data processing based on voluntary consent, the data subjects may withdraw their consent at any stage of the data processing.

Persons who are legally incapable or have limited legal capacity cannot use the Service Provider’s system through its services.

In some cases, the handling, storage, and transmission of a set of data provided are made mandatory by legislation, about which we notify the Users separately.

We draw the attention of data providers to the fact that if they do not provide their own personal data, it is the duty of the data provider to obtain the consent of the affected individual.

Personal data can only be processed for a specified purpose. The data processing must be appropriate for the purpose in every phase, and data collection and processing must be fair and lawful. Only personal data that is essential for achieving the purpose of data processing and is suitable for achieving that purpose can be processed. Personal data can only be processed to the extent and for the time necessary to achieve the purpose. The Service Provider does not use personal data for purposes different from the specified purposes.

Specific Data Processing:

7.1. Registration

Registration is not mandatory for using the application. During pre-registration, by providing a password, the User can avoid entering their data for each use and can also check their previous activities within the application.

The purpose of data processing: to facilitate and speed up the use of the application, to identify and distinguish Users.

Legal basis of data processing: the voluntary consent of the data subject, GDPR Article 6 (1) a).

Scope of personal data processed: the User’s first and last name, email address, phone number, password, and residence/place of stay.

Duration of data processing: The Service Provider processes the personal data provided by the User for as long as the User uses the application. If the User prohibits the processing of personal data or discontinues using the application, the Service Provider immediately deletes the User’s personal data.

Possible consequences of lack of registration: partial use of the application's services. Data must be re-entered for each function requiring User identification. Certain functions are only available to local residents and cannot be accessed without registration. However, some functions, such as news, municipal services, events/exhibitions/accommodations/services/shops data, locations, and online shopping functions, are available without registration.

7.2. Reporting Function

The reporting function provides registered local residents with an online platform to submit their observations to the Municipality. Registration is required to use this function. This function provides a convenient and fast reporting option for citizens to report issues (such as road surface deficiencies, public space anomalies, waste collection, etc.) to the Municipality or its institutions.

The purpose of data processing: to provide citizens with an easy and bureaucracy-free way to make reports to the Municipality or its institutions.

Legal basis of data processing: the voluntary consent of the data subject, GDPR Article 6 (1) a).

Scope of personal data processed: the User's first and last name, email address, phone number, password, residence/place of stay, and GPS coordinate.

Other processed data: the subject of the report and any attached photo.

Duration of data processing: according to the Data Processing Information for the treatment of complaints and public interest reports of the Budapest District XIII Mayor's Office, available at https://budapest13.hu.

Possible consequences of non-provision of data: the Municipality or its institution cannot effectively address the report.

If the reporting User requests the deletion of their personal data, the Service Provider deletes the data within three working days from the report, and the Municipality handles the name and contact details from the necessary personal data until the resolution of the report.

7.3. Online Sales Service (purchase of tickets, vouchers, books, audio recordings, parking tickets, etc.)

The purpose of data processing: to ensure the provision of the online sales service available in the application, to document the order, serve the order, and handle the purchase and payment, to fulfill accounting obligations, to identify the User as the purchaser, to fulfill the ordered service, to send related notifications (e.g., technical notices related to the performance, changes, cancellations, schedule changes, parking information, etc.), to process payments with the help of the payment service provider, to keep records of users, distinguish them from one another, to transfer admission data to the event organizer, to fulfill the contract.

Data Controller: the Service Provider mentioned in point I/B of this information.

Legal basis of data processing: performance of a contract, GDPR Article 6 (1) b).

Scope of personal data processed: first and last name, phone number (optional, if the purchaser provides it for receiving notifications), email address, password provided during pre-registration, shipping address if home delivery is requested.

Other processed data: transaction number, date and time, buyer code, gift voucher number, cultural voucher number.

Data deletion deadline: 210 days after the last performance in the transaction. If a legal dispute arises in connection with the purchase transaction, the Service Provider retains the data for the duration of the dispute, based on its legitimate interest, GDPR Article 6 (1) f).

Possible consequences of non-provision of data: failure of the purchase transaction.

Detailed and specific rules for sales and data processing can be found in the footer of the Jegy.hu

website.

7.4. Invoicing

The purpose of data processing: to issue an accounting document related to the purchase transactions and to retain it for the period specified by law.

Legal basis of data processing: legal obligation, GDPR Article 6 (1) c).

Scope of personal data processed: first and last name, billing address provided for the invoice, taxpayer ID for a VAT invoice (if provided by the purchaser).

Other processed data: transaction number, date, and time, invoice content.

Data deletion deadline: 8 years, or the period specified by the current tax and accounting laws.

Possible consequences of non-provision of data: failure of the purchase.

7.5. Cookie Handling and Technically Recorded Data and Statistical Data During System Operation

The data processing regulated in this point applies exclusively to the Online Sales Service (purchase of tickets, vouchers, books, audio recordings, parking tickets, etc.).

A cookie is a variable-content, alphanumeric information package sent by the server, which is stored on the User’s computer and stored for a predefined validity period. The use of cookies allows querying certain data of the visitor and tracking their internet use. Since cookies act as a kind of label that allows the site to recognize returning visitors, the use of cookies can also store usernames and passwords valid on the given site.

Temporary cookies, necessary for site usage, are session-id cookies. Their use is essential for navigating the website and for the functionality of the site. Without them, the site or its parts will not appear, browsing will become hindered, and certain functions and bank payment will not be properly realized.

While visiting the site, the User can give consent for permanent cookies to be stored on the User’s computer and accessible to the Service Provider by clicking the button on the cookie warning on the login page.

The User can set and prevent cookie-related activities using the browser program. Cookie management is generally available in the browser's Tools/Settings menu under Privacy/History/Custom Settings, labeled as cookie, or tracking. However, we reiterate that without using cookies, the User may not be able to use all the website’s services, especially payment services.

The purpose of data processing: to conduct payment transactions with the payment service provider, to identify users, to differentiate them from each other, to identify the current session of the users, to store the data provided during the session, and to prevent data loss.

Legal basis of data processing: voluntary consent, GDPR Article 6 (1) a).

Personal data processed: previously visited page.

Other processed data: ID number, date, time.

Data retention duration: temporary cookies are stored until all types of browsers are closed.

Possible consequences of non-provision of data: incomplete use of website services, failed payment transactions, failed ticket purchase.

Technically recorded data are the data generated during the use of the service by the User's login computer, and which are automatically recorded by the data controller’s system as a result of technical processes (e.g., IP address, session ID). Due to the nature of the internet, the automatically recorded data are logged automatically – without a separate statement or action by the User – by using the internet. The internet does not function without such automatic server-client communications. Except in cases where required by law, these data cannot be linked with other personal data of the User. Only InterTicket Kft., as the data controller, has access to the data. The automatically recorded log files during system operation are stored for a period justified by the need to ensure system operation.

The Service Provider may use the data for statistical purposes. The data used for statistical purposes in aggregated form must not contain any personal data of the affected User that allows identification.

7.6. Recording of Telephone Conversations

The Service Provider records incoming and outgoing telephone conversations to customer service.

The purpose of data processing: to ensure the rights of customers and the data controller, to provide evidence for resolving possible disputes, to provide evidence supporting claims that may be uncollectible, to prove agreements afterward, quality assurance, and to fulfill legal obligations.

Legal basis of data processing: voluntary consent of the data subject, GDPR Article 6 (1) a).

Scope of personal data processed: personal data provided by the subject, phone number, the audio recording of the phone conversation.

Other processed data: ID number, phone number, dialed number, date and time of the call.

Data deletion deadline: five years.

Possible consequences of non-provision of data: lack of assistance over the phone.

7.7. Customer Correspondence (Email)

If you contact our company, you can do so using the contact details provided in this information or on the website. The Service Provider deletes all incoming emails with the sender’s name, email address, date, time data, and other personal data provided in the message at most five years after data provision.

7.8. Virtual Card Application Function

The purpose of data processing: This function allows citizens to apply for a city card issued by the municipality conveniently from the application and to present the issued city card at acceptance points during approved card applications.

Legal basis of data processing: voluntary consent of the data subject, GDPR Article 6 (1) a). The Cardholder consents to the Municipality handling the data provided during the application, checking the right to use and the identity and address data in the personal and address register or by viewing the original ID and address card.

Scope of personal data processed: The user’s first and last name, email address, gender, place and

date of birth, maiden name, mother's maiden name, mobile phone number, address.

Other processed data: card number.

Data retention duration: until the cardholder returns the city card or withdraws consent to process personal data.

Possible consequences of non-provision of data: the affected person will not have a city card.

1. Web Analytics

Google Analytics, as an external service provider, helps measure website traffic and other web analytics data independently. Detailed information about the processing of measurement data can be found at the following link: http://www.google.com/analytics. The Service Provider uses Google Analytics data solely for statistical purposes and to optimize website operation.

1. Other Data Processing

For data processing not listed in this information, we provide information during data collection. We inform our customers that courts, prosecutors, investigative authorities, administrative authorities, the National Authority for Data Protection and Freedom of Information, and other bodies authorized by law may contact the Service Provider for information, data disclosure, transfer, or provision of documents. The Service Provider discloses personal data to authorities only to the extent necessary for achieving the request’s purpose, as specified by law or a binding authority order.

The person providing the data is solely responsible for the adequacy of the provided data. When entering login data, each User undertakes to use the provided data solely for their own use of the service. If the User provides someone else’s personal data, it is their duty to obtain the consent of the affected person.

The persons entitled to access personal data are employees of the Service Provider in employment or contractual relationship, employees of the courier service involved in product delivery (if the purchaser requested delivery), and the Data Processors named in this information.

IV. Data Transmission, Naming of Data Processors

1. By using the service, the User consents to the Service Provider transferring the data to the following partners. The legal basis for data transmission: performance of a contract, GDPR Article 6 (1) b).

To OJT Kft. (1139 Budapest, Váci út 99.), which performs customer service tasks. (Relevant only for purchasers who request assistance, information, or complain through the Service Provider’s customer service contact details.)

During the purchasing process, the Service Provider transfers to the selected financial institutions handling the payment those data required for processing the payment. The scope of data varies by financial institution. The personal data provided on the data request pages of financial institutions are not known by the Service Provider.

The Service Provider, as the Data Controller, is authorized and obligated to transfer any personal data at its disposal and lawfully stored to the competent authorities when required by law or a binding authority order. The Data Controller cannot be held liable for such data transfer or its consequences.

The Service Provider will only carry out data transfer not indicated above with the User’s prior and

informed consent.

V. Method of Personal Data Storage, Data Processing Security

The Service Provider’s IT systems and other data retention locations are found at its headquarters and data processors. Services provided by the Service Provider as "cloud services" are stored at the German data center of the Google Cloud Platform (FRANKFURT (europe-west3)). The data are not transferred outside the EEA.

The Service Provider selects and operates IT tools used for personal data processing during service provision to ensure that the processed data:

a) are accessible to authorized persons (availability);

b) have guaranteed authenticity and authentication (data processing authenticity);

c) have verifiable immutability (data integrity);

d) are protected against unauthorized access (data confidentiality).

The Service Provider protects the data with appropriate measures, particularly against unauthorized access, alteration, transmission, disclosure, deletion or destruction, accidental destruction, damage, and access unavailability due to technology changes.

To protect electronically managed data files in its various registers, the Service Provider ensures with appropriate technical solutions that the stored data, except when allowed by law, cannot be directly linked and assigned to the data subject.

In light of technological advancements, the Service Provider ensures data processing security with technical, organizational, and organizational measures providing an adequate level of protection corresponding to the risks associated with data processing.

During data processing, the Service Provider preserves:

a) confidentiality: protects the information to ensure only authorized persons can access it;

b) integrity: protects the accuracy and completeness of information and processing methods;

c) availability: ensures that the authorized user can access the desired information when needed, and related tools are available.

The IT systems and networks of the Service Provider and its partners are protected against computer-assisted fraud, espionage, sabotage, vandalism, fire and flood, computer viruses, computer intrusions, and other attacks. The operator ensures security with server-level and application-level security procedures.

In the automated processing of personal data, the Service Provider ensures further measures:

a) prevention of unauthorized data input;

b) prevention of unauthorized use of automated data processing systems with data transmission equipment;

c) verifiability and determination of which bodies the personal data were or may be transmitted using data transmission equipment;

d) verifiability and determination of who entered which personal data into the automated data processing systems and when;

e) recoverability of installed systems in case of malfunction; and

f) reporting of errors occurring during automated processing.

When determining and applying measures to safeguard data, the Service Provider considers the current state of technology. Among possible data processing solutions, the one providing higher protection for personal data should be chosen, except if it would cause disproportionate difficulty.

The Service Provider ensures data processing security with technical, organizational, and organizational measures providing an adequate level of protection corresponding to the risks associated with data processing.

Electronic messages transmitted over the internet, regardless of protocol (email, web, ftp, etc.), are vulnerable to network threats that may lead to unfair activity, information disclosure, or modification. To protect against such threats, the Service Provider takes all precautionary measures within its means. The systems are monitored to log all security deviations and provide evidence for all security events. System monitoring also enables verifying the effectiveness of applied precautions. However, the internet is widely known – including by the Users – to not be 100% secure. The Service Provider is not liable for potential damages caused by unavoidable attacks that occur despite the utmost care.

VI. Rights of Data Subjects

The data subject may request information about the processing of their personal data, request the correction, deletion, or withdrawal of their personal data, and exercise their right to data portability and objection as indicated during data collection or via the Service Provider’s contact details provided in point I of this Data Processing Information.

Changes in personal data or requests for data deletion can be communicated via the registered email address or a written statement sent by postal mail. Certain personal data can also be modified on the page containing the personal profile.

VI. 1. Right to Information: The Service Provider takes appropriate measures to provide data subjects with all information regarding personal data processing specified in Articles 13 and 14 of the GDPR and with each notification specified in Articles 15–22 and 34 in a concise, transparent, comprehensible, and easily accessible form, clearly and plainly worded. The right to information can be exercised in writing via the contact details provided in point I of this Data Processing Information. Upon request, information can also be provided verbally after verifying the data subject’s identity.

VI.2. Right of Access: The data subject is entitled to receive confirmation from the data controller on whether their personal data is being processed and, if so, to access the personal data and the following information:

- the purposes of data processing;
- the categories of personal data concerned;
- the recipients or categories of recipients to whom the personal data has been or will be disclosed, including recipients in third countries or international organizations;
- the anticipated retention period for the personal data;
- the right to rectification, erasure, restriction of processing, and objection;
- the right to lodge a complaint with a supervisory authority;
- information on data sources;

- the existence of automated decision-making, including profiling, and meaningful information about the logic involved and the significance and anticipated consequences of such processing for the data subject.

An email request for information – except when the data subject identifies themselves otherwise – is considered authentic by the Data Controller only if sent from the User's registered email address. The request for information should be sent to interticket@interticket.hu.

When personal data is transferred to a third country or an international organization, the data subject has the right to be informed about the appropriate safeguards relating to the transfer.

The Service Provider provides a copy of the personal data undergoing processing to the data subject. For further copies requested by the data subject, the data controller may charge a reasonable fee based on administrative costs. Upon request, the Service Provider provides information in electronic form. The data controller provides the information within one month of receiving the request.

VI. 3. Right to Rectification: The data subject may request the Service Provider to correct inaccurate personal data and complete incomplete data concerning them.

If personal data does not match the truth, and the correct personal data is available to the data controller, the data controller corrects the personal data.

VI.4. Right to Erasure: The data subject has the right to have their personal data erased by the Service Provider without undue delay if one of the following grounds applies:

- personal data is no longer needed for the purpose it was collected or otherwise processed;
- the data subject withdraws their consent on which the processing is based, and there is no other legal ground for processing;
- the data subject objects to processing, and there are no overriding legitimate grounds for processing;
- the personal data has been unlawfully processed;
- personal data must be erased to comply with a legal obligation under Union or Member State law;
- personal data was collected in connection with the offering of information society services.

Requests for the erasure or modification of personal data are fulfilled, after which the previous (deleted) data cannot be restored.

Data erasure cannot be requested if processing is necessary for one of the following reasons: compliance with a legal obligation requiring processing, legal claims by the Service Provider, or protection of another person's rights.

VI. 5. Right to Restriction of Processing: The data subject may request the Service Provider to restrict processing if one of the following conditions applies:

- the data subject contests the accuracy of personal data, in which case restriction applies for the period necessary to verify the accuracy of the data;
- processing is unlawful, and the data subject opposes erasure and instead requests restriction of use;
- the controller no longer needs the personal data, but the data subject requires it for legal claims; or
- the data subject has objected to processing; in which case restriction applies until determining whether the controller's legitimate grounds override the data subject's.

When processing is restricted, personal data may only be processed with the data subject’s consent or for legal claims or the protection of another person’s rights. The Service Provider informs the data subject in advance of the lifting of the restriction.

VI. 6. Right to Data Portability: The data subject has the right to receive their personal data provided to the controller in a structured, commonly used, and machine-readable format and to transmit this data to another controller.

VI. 7. Right to Object: The data subject has the right to object at any time to the processing of their personal data necessary for the legitimate interests pursued by the controller or a third party, including profiling. If the data subject objects, the controller may not process the personal data unless legitimate grounds override the data subject’s interests or for legal claims. If personal data is processed for direct marketing purposes, the data subject has the right to object at any time, including profiling related to direct marketing. If the data subject objects, personal data cannot be processed for direct marketing purposes.

Automated Decision-Making, Including Profiling: The data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them. This right does not apply if processing:

- is necessary for entering into or performing a contract between the data subject and the controller;
- is authorized by Union or Member State law, which lays down suitable safeguards for the data subject’s rights and interests; or
- is based on the data subject’s explicit consent.

VI. 8. Right to Withdrawal: The data subject has the right to withdraw their consent at any time. Withdrawal does not affect the lawfulness of processing based on consent before withdrawal.

Procedural Rules: The Service Provider informs the data subject without undue delay, within one month of receiving the request, of measures taken based on Articles 15–22 of the GDPR. This period may be extended by two months considering the request's complexity and number. The Service Provider informs the data subject of the extension within one month of receiving the request, stating the reasons for the delay. If the data subject submitted the request electronically, information is provided electronically unless requested otherwise.

If the Service Provider takes no action on the data subject’s request, it informs the data subject without delay, within one month of receiving the request, of the reasons for inaction and the right to lodge a complaint with a supervisory authority and seek judicial remedy.

The Service Provider provides requested information and notification free of charge. If the data subject’s request is clearly unfounded or excessive, especially due to its repetitive nature, the Service Provider may charge a reasonable fee based on administrative costs or refuse the request.

The Service Provider informs all recipients of corrections, erasure, or restriction unless impossible or involves disproportionate effort. Upon request, the Service Provider informs the data subject of the recipients.

The Service Provider provides a copy of personal data undergoing processing to the data subject. For further copies requested, the Service Provider may charge a reasonable fee based on administrative costs. If the data subject submitted the request electronically, information is provided electronically unless requested otherwise.

VI. 9. Right to Compensation and Redress: Any person who suffers material or non-material

damage resulting from a breach of the GDPR has the right to receive compensation from the controller or processor for the damage suffered. The processor is only liable for damages caused by processing if it has not complied with specific legal obligations or disregarded or acted contrary to lawful instructions from the controller. If multiple controllers or processors, or both, are involved in the same processing and are liable for damages, each is jointly and severally liable for the total damage. The controller or processor is exempt from liability if it proves it is not responsible for the damage-causing event.

VII. Legal Remedies

For questions or comments, contact the Data Protection Officer using the contact details provided in point I of this Data Processing Information.

Right to Judicial Remedy: The data subject may bring proceedings against the controller for violating their rights. The court proceeds without delay. The data subject may choose to file a claim with the court of residence (permanent address) or place of stay (temporary address). Contact details for the court can be found at http://birosag.hu/torvenyszekek.

Data Protection Authority Procedure: A complaint can be filed with the National Authority for Data Protection and Freedom of Information:

Name: National Authority for Data Protection and Freedom of Information

Address: 1125 Budapest, Szilágyi Erzsébet fasor 22/C.

Mailing address: 1530 Budapest, Pf.: 5.

Phone: 06.1.391.1400

Fax: 06.1.391.1410

Email: ugyfelszolgalat@naih.hu

Website: http://www.naih.hu

APPENDIX

Definitions Used in this Data Processing Information

Personal Data: Any information related to an identified or identifiable natural person (“data subject”). An identifiable natural person is one who can be identified, directly or indirectly, particularly by reference to an identifier such as a name, ID number, location data, online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

Data Processing: Any operation or set of operations performed on personal data or sets of personal data, whether automated or not, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

Restriction of Data Processing: The marking of stored personal data to restrict future processing.

Profiling: Any form of automated processing of personal data consisting of the use of personal

data to evaluate certain personal aspects relating to a natural person, particularly to analyze or predict aspects concerning the natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

Data Controller: The legal entity that determines, alone or jointly with others, the purposes and means of the processing of personal data.

Data Processor: The legal entity that processes personal data on behalf of the controller.

Recipient: A natural or legal person, public authority, agency, or other body to whom personal data is disclosed, whether a third party or not.

Third Party: A natural or legal person, public authority, agency, or body other than the data subject, controller, processor, or persons authorized to process personal data under the controller’s or processor’s direct authority.

Data Subject’s Consent: The data subject’s freely given, specific, informed, and unambiguous indication of their wishes, by which they signify agreement to personal data processing concerning them by a statement or clear affirmative action.

Data Processing: The performance of technical tasks related to data processing operations, regardless of the method and tool used for execution and the place of application, provided the technical task is performed on the data.

Data Deletion: Rendering data unrecognizable so that recovery is no longer possible.

EEA State: An EU member state, a state party to the EEA Agreement, and a state whose citizen has the same status as an EEA state citizen based on an international agreement between the EU, its member states, and a non-party state.

Data Subject: Any identified or identifiable natural person based on personal data.

User: The natural person who registers or purchases without registration on the Service Provider’s website.

Third Country: Any state that is not an EEA state.

Disclosure: Making personal data available to anyone.