Privacy policy
Download in .pdf
Effective from 01.01.2021

I. Data Controller (Service Provider)

Service Provider's Name:	InterTicket Kereskedelmi Kft.
Seat and Postal Address:	1139 Budapest, Váci út 99. HUNGARY
Registration Authority:	Metropolitan Court acting as Registry Court
Company Registration Number:	Cg. 01-09-736766
Tax number:	10384709-2-41
E-mail address:	ors.orszagh@interticket.hu
Website:	interticket.co/smartcity
Call Centre:	+36-30-9222-002
Customer Service e-mail address:	ors.orszagh@interticket.hu
Location and Contact for Complaints:	1139 Budapest, Váci út 99. HUNGARY +36-30-9222-002 ors.orszagh@interticket.hu Weekdays between 10.00 and 16.00
Name of Data Storage Provider:	
Address of Data Storage Provider:	
Data Protection Identifier:	NAIH-54216/2012.
Data Protection Officer's phone number:	266-0000 / 327-es mellék
Data Protection Officer's e-mail address:	adatvedelmi.tisztviselo@interticket.hu

II. Privacy policy employed by the Company

2. Information regarding management of data by Service Provider is continuously available in the footer of the starting page of the Jegy.hu website operated by the Service Provider.
3. Service Provider reserves the right to modify the Prospectus on Data Management unilaterally. In the event of modification, Service Provider shall notify the User by publishing the changes on the interticket.co/smartcity website. User accepts the revised Prospectus on Data Management by using the service after the modification takes effect.
4. In order to protect the personal information of its customers and partners, Service Provider considers it important to respect its clients` right to information self-determination. Service Provider shall treat the personal data in a confidential manner and shall apply all security, technical and organizational measures that guarantee the security of data. Service Provider's data management practices are contained in this Prospectus on Data Management.
5. Service Provider's principles on privacy are in line with the current data protection legislation, thus especially with the following:
- Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (hereinafter referred to as Privacy Act);
- 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, GDPR);
- Act V of 2013 on the Civil Code (Civil Code);
- Act C of 2000 on Accounting (Accounting Act);
- Act CXXXVI of 2000 on the Prevention and Combating of Money Laundering and Terrorist Financing (PCMLTF);
- Act CVIII of 2001 on Certain Aspects of Electronic Commerce and Information Society Services (E-Commerce Act);
- Act XLVIII of 2008 on the Basic Requirements and Certain Restrictions of Commercial Advertising Activities (Business Advertising Act).
6. Service Provider shall only use personal information based on the legal basis included in the GDPR and solely for the specified purpose.
7. Service Provider is committed that before collecting, recording or handling any personal data of its customers it will publish clear, soliciting Customers' attention and unambiguous statements which inform Customers of the ways their data is recorded, their purpose and principles. If providing personal data is compulsory by law, the relevant rules and regulations must also be indicated. Those involved must also be informed of the purposes of data processing and by whom the personal data will be handled and processed.
8. If the Company intends to use the personal data provided for purposes other than it was originally provided for, the Company must inform the customer and obtain their express, prior consent and make it possible for the customer to prohibit such use.

III. The legal basis and purpose of data processing, the scope of the processed data, length of data processing, entities entitled to learn personal data

1. Service Provider`s data processing is based on the following legal rights (Paragraph 1 of Section 6 of the GDPR):
a) the individual has given their consent to the processing of their personal data for one or more specific purpose (voluntary consent);
b) data processing is necessary for the fulfilment of such a contract where the affected person is one of the parties or if it necessary to carry out steps required by the affected person before the contract is entered into (fulfilment of the contract);
c) data processing is necessary to fulfil the legal obligation for the data controller (legal obligation);
d) data processing is necessary to validate legitimate interest of data controller or a third party (legitimate interest).
2. In case of data processing based on voluntary consent the affected person may withdraw their consent at any time during data processing.
3. Individuals with particular disabilities and children with limited ability may not use services via Service Provider`s system.
4. In some cases processing, storage and forwarding are made mandatory by law of which we will notify users separately.
5. Please note that if data provider is not providing their own personal data, it is their responsibility to obtain the consent of the person concerned.
6. Personal data may only be handled for a specific purpose. The purpose of data management must be met, data entry and management must be fair and legitimate at all stages of data processing. Only personal data that is essential for achieving the purpose of data processing can be handled to achieve this goal. Personal data can only be handled to

the extent and for the duration required to achieve the goal. Service Provider will not use personal data for purposes other than those indicated.

7. Electronic newsletter

Purpose of data processing: Sending email newsletters containing advertisements to interested users. If user subscribes to the newsletter, Service Provider can send newsletters at a frequency at its own discretion. Service Provider shall endeavour to offer events relevant to the reader of the newsletter based on user`s place of residence, previous purchases and other data collected through profiling.
Grounds for data processing: voluntary consent of the affected person, subsection a) Paragraph 1 of Section 6 of the GDPR.
Scope of processed data: name, email address, post code, phone number and data collected through profiling.
Deadline to erase data: Data provided will be handled by Service Provider until such time as User prohibits use for this purpose by unsubscribing. To unsubscribe from the newsletter, click the Unsubscribe link at the bottom of the newsletter. The personal data will be deleted within 10 working days of receiving this request.
Possible consequences of failure to provide data: User is not notified of the events.

8. Statistics

Data controller can use the data for statistical purposes. The use of data in a statistically aggregated form cannot contain the name or any other identifiable information of the user in any form.

9. Service Provider`s correspondence with customers (email)

If you would like to contact our company you can get in contact with Service Provider on the contact details provided in this information leaflet or via the contacts specified on the website. Service Provider deletes all received emails, together with sender`s name, email address, date, time and other personal data provided in the email no later than 5 years after the disclosure.

10. Web analytics

Google Analytics as an external service provider helps to independently measure website visits and other web analytics data. For detailed information on how measured data is handled please visit the following link: http://www.google.com/analytics. Google Analytics data is used by the Service Provider for statistical purposes only to optimize the functionality of the site.

11. Other data management

We provide information on data management not specified in this document at the time of the registration of such data. Please note that the court, prosecutor, investigating authority, offense authority and administrative authority, National Authority for Data Protection and Freedom of Information, Hungarian National Bank as well as other bodies under the authorization of the legislation may request Service Provider to provide information, provide and hand over data or provide documents. Service Provider shall only disclose personal information to the authorities – if the authority has specified the exact purpose and the scope of data – to the extent necessary for the purposes of the request.

12. Data controller shall not check the provided personal information. The person providing the information will be solely responsible for the compliance of the provided information. When Users provide their email address, they assume responsibility that only they will use

the Service from this email address. In this respect the person who registers the email address will be responsible for every login used with the given email address. If User is not providing their own personal data, they have the duty to obtain consent from the affected person.
13. People in the employment of or in contractual relationship with Service Provider, employees of the courier company arranging the delivery of the products as well as the data processors will be entitled to get to know the personal data.

IV. The method of storing personal data, security of processing

1. Service Provider`s IT systems and other data retention systems are located at its own seat and at its data processors`.
2. Service provider selects and manages the IT tools used to manage personal data in the provision of the service so that the data:
a) is available for those entitled (availability);
b) authenticity and validation is provided (data authenticity);
c) integrity can be verified (data integrity);
d) is protected against unauthorized access (data confidentiality).

3. Service Provider will protect the data with appropriate measures, especially against unauthorized access, alteration, transmission, disclosure, deletion or loss, as well as accidental destruction, harm, as well as unavailability due to any change to the technology used.
4. In order to provide security to the data stored electronically in its various registers, Service Provider shall ensure, by using suitable technology, that the stored data could not be directly linked and linked to the data subject, unless permitted by law.

5. Service Provider will employ such technical, structural and organizational measures to defend the security of data management that provides appropriate level of security to the risks arising in connection with data management.
6. During data processing Service Provider shall maintain:
a) confidentiality: to protect information so that only persons authorized are able to aces it;
b) integrity: to protect accuracy and totality of information and method of processing;
c) availability: to ensure that if eligible user needs it, they can actually access the required information and have the tools available for such.

7. Service Provider's IT System and network, as well as its partners`, are protected against computer-assisted fraud, espionage, sabotage, vandalism, fire, flood, furthermore against computer viruses, cyber intrusions and attacks leading to refusal of Services. Service Provider uses server-level and application-level protection features to ensure security.

8. In the automated processing of personal data, Service Provider provides additional measures
a) to prevent unauthorized data entry;
b) to prevent the use of automatic data processing systems by unauthorized persons by means of data transmission devices;

c) verifiability and determination of which bodies personal data has been or may be transmitted to by means of data transmitting equipment;
d) verifiability and determination of when and who entered which personal data into the automatic data-processing systems;
e) the recoverability of installed systems in case of malfunction and
f) report are prepared on errors occurring during automated processing.
9. Service Provider shall take into account the prevailing development of technology when determining and applying measures for data security. If there are several possible solutions for data processing, the one that ensures the highest possible protection of personal data must be chosen unless this would be disproportionate.
10. Service Provider shall ensure the protection of data procession security by such means of technical, organizational and institutional measures that provide a level of protection appropriate to the risks associated with data processing.

11. Electronic messages transmitted via the Internet are vulnerable to network threats irrespective of protocol (email, web, ftp, etc.) which may result in fraudulent activity or disclosure or modification of information. Service Provider shall take all reasonable precautions to protect from such threats. Service Provider shall monitor the Systems in order to record any security deviation and to provide proof in case of all security related events. However, the Internet is commonly – therefore, also to the User – known to be not one hundred percent secure. Service Provider shall not be responsible for damages caused by inevitable attacks despite its best efforts.

V. Data subjects` rights
1. Data subject may request information on the use of their personal data, furthermore may request correction and, with the exception of compulsory data processing, erasure or revocation of such, may exercise their right to recording and to object as indicated at the time of data recording a well as via the contacts of Service Provider specified in Section 1 of the present document.
Requests for changes in personal details or for deleting personal details can be sent from the registered email address or by post, via a written, fully conclusive private document expressing such request. Certain personal data can also be modified using the website's personal profile page.
2. Right to be informed: Service Provider shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The information shall be provided in writing via the contacts specified in section I of the present Information on Data Processing document. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.
3. Right of access by the data subject: The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:
- purposes of the processing;
- the categories of personal data concerned;

- the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
- the envisaged period for which the personal data will be stored
- the right to request rectification or erasure or restriction of processing of personal data;
- the right to lodge a complaint with a supervisory authority;
- any available information as to the source of data;
- the existence of automated decision-making, including profiling, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Data Controller shall only see credible any information request sent by email – unless the person concerned otherwise identifies the credibility – if the request is sent from the User`s registered email address. Request for information must be sent via email to interticket@interticket.hu address.

4. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards relating to the transfer.

5. The Service Provider shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the data controller may charge a reasonable fee based on administrative costs. Service Provider shall provide information to data subject by electronic means. Information shall be provided within a maximum of one month from the request.

6. Right to rectification: Affected person may request from Service Provider to rectify or complete the processed personal data.

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

7. Right to erasure: The data subject shall have the right to obtain from the Service Provider the erasure of personal data concerning him or her without undue delay where one of the following grounds applies:

- the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;;
- the data subject withdrew consent on which the processing is based and where there is no other legal ground for the processing;
- the data subject objects to the processing and there are no overriding legitimate grounds for the processing;
- the personal data have been unlawfully processed;
- the personal data have to be erased for compliance with a legal obligation in Union or Member State law;
- the personal data have been collected in relation to the offer of information society services.

The previous (erased) data can no longer be recovered after the request for erasure or modification has been completed.

8. Erasure of the data cannot be requested if the processing is necessary for either of the following reason: for compliance with a legal obligation which requires processing by Union or Member State law or if the data are needed for the establishment, exercise or defence of legal claims of Service Provider.

9. Right to restriction of processing: The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:
- the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
- the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
- the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; or
- the data subject has objected to processing; in this case restriction shall apply for a period enabling the verification whether the legitimate grounds of the controller override those of the data subject.

10. Where processing has been restricted, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person. The data subject shall be informed by the Service Provider before the restriction of processing is lifted.

11. Right to data portability: The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller.

12. Right to object: The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her, including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

13. Automated individual decision-making,including profiling: The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. The above right shall not apply of the data processing
- is necessary for entering into, or performance of, a contract between the data subject and a data controller;
- is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
- is based on the data subject's explicit consent.

14. Right to withdrawal: The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal.

15. Procedural rules: Service Provider shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The Service Provider shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

16. If the Service Provider does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

17. Service Provider shall provide the requested information and any communication free of cha Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the Service Provider may charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested or refuse to act on the request.

18. The Service Provider shall communicate any rectification or erasure of personal data or restriction of processing carried out to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

19. The Service Provider shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the Service Provider may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

20. Compensation and grievance money: Any person who has suffered material or non-material damage as a result of an infringement of the data protection regulation shall have the right to receive compensation from the controller or processor for the damage suffered. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of the data protection regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller. Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage. A controller or processor shall be exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage.

VII. Law enforcement options:

1. For questions and comments please contact the Data Protection Officer at the contact details specified in section I of this Information on Data Processing document.
2. Right to Court: In case of infringement of his or her rights the data subject may bring these to the attention of the court. The court shall hear the case without delay.
3. Data Protection Authority procedures: Complaints may be made to the National Authority for Data Protection and Freedom of Information.

Name: National Authority for Data Protection and Freedom of Information
Seat: 1125 Budapest, Szilágyi Erzsébet fasor 22/C.
Postal address: 1530 Budapest, Pf.: 5.
Phone: 06.1.391.1400
Fax: 06.1.391.1410
Email: ugyfelszolgalat@naih.hu
Website: http://www.naih.hu

ANNEX

Definitions used in the present Information on Data Processing document

1. personal data: means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
2. processing: means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
3. restriction of processing: means the marking of stored personal data with the aim of limiting their processing in the future;
4. profiling: means 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, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
5. controller: means the legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data;
6. processor: means a legal person which processes personal data on behalf of the controller;
7. recipient: means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not;
8. third party: means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;
9. consent: of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear

affirmative action, signifies agreement to the processing of personal data relating to him or her;
10. data processing: carrying out technical tasks connected to data processing operations, irrespective of the method and tool used to carry out this operations as well as the place of application, provided that the technical task is carried out on the data;
11. data erasure: making the data unrecognizable in such a way that they may not be restored;
12. EEA country: a member state of the European Union and another state party to the Agreement on the European Economic Area, as well as a state the national of which enjoy the same legal state as a citizen of the state party to the Agreement on the European Economic Area on the basis of the agreement between the European Union and its member states and a state not party to the Agreement on the European Economic Area;
13. data subject: any specified natural person identified or – directly or indirectly – identifiable by personal data;
14. customer: any natural person who registers on the website of Service Provider or carries out a purchase without registration:
15. third country: any stat the is not a member of the EEA;
16. disclosure: making personal data available for anyone.