PRIVACY POLICY

I. Legal Background and Purpose of our Privacy Policy. The Data Controller. For the purpose of drafting these rules, special attention was made to the provisions of Act CXII of 2011 on Informational Self-determination and Freedom of Information, and Act VI of 1998 on the promulgation of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe of 28 January 1981 and the recommendations of the "ONLINE PRIVACY ALLIANCE".

This Privacy Policy and any issues related to data protection shall be governed by Hungarian law. In the event of any legal disputes arising in connection with data protection issues, the courts having competence according to the registered office of the Data Controller shall have exclusive jurisdiction.

The purpose of this Privacy Policy is to ensure in every field of our services and for every individual, that the rights and fundamental civil liberties, hence in particular the right to privacy, of the individuals, regardless of their nationality or domicile, are respected in the course of automatic processing of their personal data (data protection).

Particulars of the Data Controller:

Flight Refund Kft.

registered office: 1024 Budapest, Rózsahegy utca 1-2. 1. em. 1.

Company registration number: 01-09-197506

(hereinafter as: Data Controller)

II. Definition of the Terms Related to Personal Data

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

sensitive data: shall mean the personal data relating to ethnic origin, nationality, political opinion or political affiliations, religious or other ideological convictions, membership in any interest groups, sexual life,personal data relating to health or pathological addictions and personal criminal data;

data management: shall mean, regardless of the given process applied, any operation or the entirety of operations made with respect to the data, thus in particular the collection, entry, recording, systematisation, storage, alteration, usage, retrieval, forwarding, disclosure, synchronisation, matching, blocking, deletion or destruction of the data, furthermore the prevention of further usage of the data, making of pictures, sound or image recordings, or the recording of physical characteristics suitable to identify the given person (e.g. fingerprints or palmprints, DNS samples, iris image);

data processing: shall mean the performance of the technical tasks related to the data management operations, regardless of the method applied and the tools used for such

operations, or the place of application, provided that the technical tasks are executed on the data;

data transmission: when the data is made available to a specific third party;

public disclosure: when the data is made available to everyone;

data controller: shall mean the natural person or legal entity or organisation without legal personality, that individually, or together with others, sets the purpose of data management, takes and implements decisions regarding data management (including the devices used), or enforces the implementation thereof by the data processor appointed by him

data processor: shall mean the natural person or legal entity or an organisation without legal personality that processes the data on the basis of a contract (including any contract concluded pursuant to provisions of law)

deletion of data: shall mean the act of making the data unrecognisable so that their recovery is impossible.

III. Principles of Data Management

1. data can only be obtained and processed in a fair and lawful way;

2. data can only be stored for the defined and lawful purposes and shall not be used in a way contrary to these purposes;

3. the data shall be proportionate to the purpose of their storage and shall meet such purpose and may not extend beyond such purpose;

4. the data must be accurate and, if necessary, up-to-date;

5. the method of data storage must ensure that the data subject can be identified based on the given data only for the time required for the purpose of storage;

6. the personal data relating to racial origin, political opinion, religious or other convictions, health or sexual life shall not be processed with automatic (machine based) processing, except when Hungarian law provides appropriate guarantees. The same shall apply to personal data related to criminal convictions as well,

7. appropriate security measures must be made to protect the personal data stored in automated data sets in order to prevent accidental or unlawful destruction or accidental losing or unlawful access, alteration or distribution.

IV. Further Guarantees Protecting the Data Subjects

Everyone has the right to

1. obtain knowledge about the automated set of personal data, the main purposes thereof, and the persons managing such data and their customary domicile or registered office;

2. obtain information, at reasonable intervals and without excess delay or costs, whether their personal data are stored in an automated data set or not, and also to be informed about these data in a manner comprehensible for them;

3. have these data corrected or deleted, if required, in the simplest and fastest way possible;

4. have recourse to legal remedy if their request for information or (if justified) for disclosure, correction or deletion, as stipulated by law, is not performed. At the data subject's request, the data controller shall provide information about the data handled by it or processed by the data processing entity commissioned by it, the purpose of data management, its legal grounds, duration, the name, address (registered office) and data management related activities of the data processing entity, furthermore about the persons and/or entities that received the data and the purpose thereof. The data controller shall provide the requested information in a clear and comprehensible form, in writing, as soon as possible, but in no event later than within 30 days from submission of the respective request. The data subject, if their rights are violated, can turn to the court for action against the data controller. The data controller shall be obliged to compensate the damages caused to any party as a result of unlawful management of the data subject's data or violation of the technical data protection requirements. The data controller shall be liable *vis-á-vis* the data subject concerning the damages caused by the data processor as well. The data controller shall be released from its liability if it proves that the damage occurred due to an unavoidable cause beyond the scope of data management. The part of the damage which was caused by the intentional or grossly negligent conduct of the aggrieved party shall not be compensated.

Personal data may be handled if:

1. the data subject provided his/her consent to that, or

2. any piece of legislation or a local government's decree (pursuant to an authorisation granted under law) orders data management, within the scope and to the extent stipulated by law. The public disclosure of personal data may be ordered by law for public interest, by specifying the exact scope of data. In all other cases, the consent of the data subject (their written consent in case of sensitive data) shall be required for public disclosure. In the event of any doubt, it shall be presumed that the data subject did not provide their consent. The data subject's consent (permission) shall be deemed as granted regarding those personal data which were disclosed by the data subject during their public appearance or released by them for publication.

Sensitive data may be handled if:

1. the data subject provided his/her written consent regarding data management, or

2. if (with regards to the personal data relating to racial origin, the fact of belonging to national or ethnic minorities, political opinion or political affiliations, religious or other ideological convictions, membership in any interest groups) the data management is based on international conventions or is ordered by law to enforce any fundamental rights guaranteed under the Basic Law of Hungary (Fundamental Law) or for the sake of national security, prevention of crime, or criminal prosecution;

3. data management is required by law in other cases.

The rules pertaining to data management and protection of the personal data of visitors shall be applied only and exclusively for natural persons, since the term “personal data” can only be interpreted and applied for natural persons (pursuant to Act CXII of 2011 on Informational Self-determination and Freedom of Information), therefore this Privacy Policy shall be binding only in terms of the handling of personal data of the natural persons using the https://flight-refund.eu (hereinafter as: homepage).

Data management being tied to a specific purpose:

Personal data can only be managed for a specific purpose, in order to exercise a right or perform an obligation. Data management must comply with the above purpose in every phase of the process. Only such personal data can be managed that is indispensable for the achievement of the purpose of the data management, suitable for achieving such purpose, only to the extent and for the duration required for achievement of the purpose.
Purpose of data management: to provide services related to prefer a claim, the fulfilment of the related rights and obligations, prepare visitor statistics, ensure access to data for the other users, in other words to ensure the highest possible service level and most efficient services, furthermore to use the data (if consent to this purpose has been granted) for marketing purposes, sending of newsletters (commercial offers), direct marketing purposes.

Scope of managed data: data provided by the users on the homepage: (name, mother’s name, address, e-mail, place of birth and date, bank account number)

DataSecurity:
The data controller, and in its scope of activity, the data processor as well, shall ensure the security of the data, furthermore shall take all technical measures and make all arrangements and apply all procedural rules necessary to ensure proper data protection required under the Data Protection Act and the other data protection and confidentiality and privacy rules. The data must be protected, in particular against unauthorized access, alteration, disclosure, deletion, damage or destruction.

V. Data Protection Principles

The Data Controller undertakes the obligation that prior to taking or recording or handling any data of its users, it shall display a clear and unambiguous warning notice (Privacy Policy) whereby the user shall be informed on the method, purpose and principles of data recording. In addition to this, the Data Controller shall call the attention of the user to the voluntary nature of data provision. The data subjects must be informed of the purpose of data management, and about the persons or entities that will handle and process the data. Every employee and executive officer of the Data Controller shall have the right to get to know the data managed by the Data Controller. The provision of information on the fact of data management shall be deemed as duly performed also when law orders the recording of data (via transmission or coupling of the data) already handled.

In every case when the Data Controller intends to use the provided data for a purpose other than the original purpose of data recording, it shall be obliged to inform the users thereof and obtain their express prior consent and also allow them the opportunity to forbid such use.

In the course of recording and handling the data, the Data Controller shall observe the limitations defined under the principles in all cases, and shall inform the data subjects about its activity, if requested, via electronic mail. The Data Controller undertakes the obligation to refrain from enforcing any sanctions against users who refuse to perform any non-compulsory data provision.

Data Controller shall be managed the data of users under the age of 18 years parallel the consent of their parents only.

Data Controller undertakes the obligation to ensure data security, and make all technical and organisational measures and adopt such procedural rules that guarantee that the recorded, stored and handled data are protected, and also to prevent destruction, unauthorized use and unauthorized alteration of such data. It also undertakes to call upon any third parties to whom it possibly transmitted or delivered the data to comply with these obligations.

Data and information suitable to identify a person shall mean those personal data of natural persons with which someone can be personally identified or which allow to create a communicational contact with someone or to define the physical location of someone, including, but not limited to the following: name, phone number, e-mail address.

The following shall not be considered as personal data: anonymous information that cannot be used for personal identification and cannot be linked to any natural persons, and those demographic data that are collected in such a way so that they are not linked to the personal data of identifiable persons and therefore no connection with a natural person can be established.

As a general principle, every time we request personal data from our users, after reading and interpreting the necessary informational text, the users can freely decide whether they provide the requested information or not. However, it needs to be underlined that should someone not provide their personal data, this may result in not being able to use the given service, the use of which is subject to provision of personal data.

This Privacy Policy is relating to the protection of the non-public personal data of the users made available to the Data Controller. If anyone publishes their personal data or any part thereof voluntarily, such information shall not be covered by the Privacy Policy.

Without the respective authorisation, under no circumstances shall we deliver the personal data provided to us by our users to any third parties.

In the event the duly authorised authorities request Data Controller to deliver certain personal data in the proper manner stipulated by law (e.g.: based on suspicion of a crime, via an official data seizure decision), meeting its statutory obligation, shall deliver the requested information available to it.

When our users deliver personal data to us, we shall make each and every necessary measure to ensure that these data are protected and secure, both during network communications (i.e. during online data management) and in the course of storage of the data (i.e. offline data management).

The Data Controller shall ensure that the visitors can access, correct and supplement their own personal data via those communication channels and by using the same options, which were made available to them when they provided to us their personal data previously. In this way we would like to guarantee that the personal data of our users are always up-to-date and accurate. Should any of our users ask for deletion of their personal data from our system (obviously, in certain cases the given user must accept that from that time on they will not be able to use the given service to which the given data belonged, or at least not in the same way), we shall fulfil this request immediately. Data retention time go on at the fulfilment of the purpose.

VI. Subject to the above provisions, the Data Controller shall apply the following rules in the course of data collection:

The information automatically logged by our servers. Our servers automatically register our users' operating system. We use these information only and exclusively in an aggregated and processed manner, for purposes of eliminating any possible errors in our services, to improve the quality of service and for statistical purposes. Data are not coupled or linked to any other data provided by the users in any way whatsoever.

Data suitable to contact the individual users. We use data suitable to contact the individual users (such as e-mail addresses) only and exclusively for the purposes approved by the User in advance, and under no circumstances shall we deliver such data to third parties without the User's prior written permission, save for the exceptions stipulated by law.

Data suitable to contact the individual users physically. We shall use the data only and exclusively for the purposes approved by the User in advance, and we shall not deliver such data to third parties, save for the exceptions stipulated by law.

User give your consent, that the Data Controller transmit data provided by the users on the homepage for PannonHitel Zrt. (1024 Budapest, Rózsahegy u. 1.) sets in services related to prefer a claim. We use data suitable to contact the physically users. User in advance, and under no circumstances shall we deliver such data to third parties without the User's prior written permission, save for the exceptions stipulated by law.

VII. At the User's request, the Data Controller shall provide information about the User's data handled by it, the purpose of data management, its legal grounds, duration, the name, address (registered office) and data management related activities of the data processing entity, furthermore about the persons and/or entities that received the data and the purpose thereof.

Should our users deem that we have violated their right to protection of their personal data, they can file their claims to court, or seek the assistance of the Authority for Data Protection and Freedom of Information (1125 Budapest, Szilágyi Erzsébet fasor 22/c, www.naih.hu).
The court shall hear the case in an accelerated procedure. The judgement on the legal action shall fall within the competence of the regional courts. At the User's (data subject) discretion, the legal action can be started at the regional court having competence according to the user's (i.e. the data subject) domicile or habitual residence as well.

The detailed statutory provisions governing legal remedies and the obligations of the data controller are stipulated by Act CXII of 2011 on Informational Self-determination and Freedom of Information.

Data protection ID: Flight Refund Kft.: NAIH-131496/2017