Data Management and Data Security Policy

TrustAir Aviation Korlátolt Felelősségű Társaság

1 Introduction

The purpose of this Privacy and Data Security Policy ("**Policy**") of TrustAir Aviation Korlátolt Felelősségű Társaság ("**Data Controller**") is to provide data subjects ("**Data Subject**") with detailed and exhaustive information in accordance with the applicable legal requirements on the scope of their personal data processed by the Controller, the purposes and methods of data processing and all other facts related to the processing of their data, in particular, but not limited to, their rights in relation to the processing and possible remedies. This Policy is also intended to regulate the legal, technical, security and other conditions and requirements for the processing activities carried out by the Controller.

2 Data controller's services, data, data protection manager and data protection officer

2.1 The Data Controller processes personal data in the course of the following services:

2.1.1 Patient air transport

Arranging and carrying out air transport of patients from abroad by special air ambulance aircraft or commercial flights, in accordance with requests from the Intermediary (assistance providers, insurers) or the Data Subject (or their relatives).

2.1.2 Business travel

The Data Controller may arrange convenient and fast travel for Data Subjects and their business partners using its own aircraft, if required.

2.1.3 Cargo

The Data Controller may arrange the delivery of various consignments and parcels by air as a matter of urgency.

2.1.4 Patient care

In specific cases, the Data Controller will arrange for full treatment in accordance with the Data Subject's needs and the condition of their illness, which may include the organization of professional patient transport, full care or treatment.

2.1.5 Healthcare education

The Data Controller's staff may provide general first aid courses: in the form of small group lectures, interactive demonstrations with tools and/or practical training.

2.1.6 Advising Services

The Data Controller advises enquirers on its activities in the fields of medical and emergency aviation, health systems development, helicopter aviation and aircraft operations.

2.2 Data Controller's data

name: TrustAir Aviation Korlátolt Felelősségű Társaság

registered seat: 9099 Pér, Petőfi utca 1.

e-mail: info@trustair.hu

2.3 Data Protection Manager of the Data Controller

The Data Protection Manager of the Data Controller shall ensure compliance with this Policy and the procedures relating to the protection and processing of personal data at the Data Controller and shall also act as the contact person of the Data Controller for all matters and questions relating to the processing of personal data by the Data Controller. Name and contact details of the Data Protection Officer of the Controller:

name: Tóth Réka

e-mail: toth.reka@trustair.hu

2.4 Data Protection Officer

The Data Protection Officer of the Data Controller at the time of adoption of this Policy:

name: RVD Partners Consultancy Limited Liability Company

head office: 1055 Budapest, Honvéd utca 18.

data protection officer person: dr. Sallai Fruzsina

e-mail: dpo@trustair.hu

3 Legislation affecting the Data Controller's processing

3.1 The legal background of the Data Controller's processing:

- Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Regulation (EC) No 95/46/EC ("**GDPR**");
- Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information ("**Info Act.**");
- Act CLIV of 1997 on Health Care ("**Health Care Act**");
- Act XLVII of 1997 on the processing and protection of healthcare data and related personal data ("**Eüak Act**");

- Decree 62/1997 (XII. 21.) NM on certain issues of processing of health and related personal data ("**Eüak.ord.**");
- Act XCVII of 1995 on Air Transport ("**AT Act**");
- Government Decree No 25/1999 (II. 12.) on the Rules of Air Passenger Transport ("**Air Passenger Transport Decree**");
- Act V of 2013 on the Civil Code ("**Civil Code**")
- Act C of 2000 on Accounting ("**Accounting Act**");
- Act CL of 2017 on the Rules of Taxation ("**Taxation Act**")

4 Concepts and definitions relating to the Controller's service and data management

"**personal data**" shall mean 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, number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

'**controller**' shall mean the natural or legal person or unincorporated body which, alone or jointly with others, determines the purposes for which the data is to be processed, makes and executes decisions regarding the processing (including the means used) or has them executed by a processor, within the limits set by law or by a legally binding act of the European Union;

"**processing**" shall mean any operation or set of operations which is performed upon personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

"**special categories of personal data**" shall mean any data that falls within special categories of personal data, namely personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union memberships, genetic data, biometric data revealing the identity of natural persons, health data and personal data concerning the sex life or sexual orientation of natural persons;

"**medical treatment**" shall mean any activity aimed at preserving health and the direct examination, treatment, care, medical rehabilitation or processing of the examination material of a person concerned, for the purpose of preventing, detecting, diagnosing, curing, maintaining or improving the level of deterioration of the condition resulting from a disease, including the supply of medicines, medical aids, medical care, rescue and ambulance services and obstetric care (Section 3. paragraph c) of Eüak.tv.);

"**medical record**" shall mean a record, register or any other form of data containing medical and personal identification data, irrespective of its medium or form, which is disclosed to the patient's care provider during the course of treatment (Section 3, paragraph e) of the Health Care Act).

"**patient care provider**": shall mean a medical doctor, health care professional, other person carrying out activities related to the treatment of the person concerned, a pharmacist (Section 3 paragraph g) of the Health Care Act);

"**health-related data**": shall mean personal data belonging to the group of special (sensitive) data under the provisions of the Info Act, which, due to its quality, is entitled to special protection;

"**health data**" shall mean any data relating to the physical, mental or psychological state, pathological condition, pathological addiction, and the circumstances of the illness or death, the cause of death of the data subject, as communicated by him or her or by another person, or as observed, tested, measured, mapped or derived by the healthcare network; and any data relating to or affecting any of the foregoing (e.g. behavior, environment, occupation);

"**personal identification data**" (in the context of health): shall mean personal data used to identify the data subject of health data, which are processed by the controller together with the health data as part of the health record for the same purpose as or inseparable from the processing of the health data (Section 3/B of the Health Care Act);

"**the data subject's consent**" means a freely given, specific, informed and unambiguous indication of the subject's intention by which the data subject signifies, by a statement or by any other such act expressing their unambiguous consent, in order to signify their agreement to the processing of personal data concerning them;

"**close relative**" shall mean spouse, relative in the direct line, adopted, step- and foster child, adoptive, step- and foster parent, brother, sister and partner;

"**transport report**": shall mean a report of the transport of the patient and their medical records from the sending hospital to the receiving hospital. The transport report is part of the medical record.

"**data processor**" shall mean a natural or legal person or an unincorporated body which processes personal data on behalf of or under the instructions of the controller, within the limits and under the conditions laid down by law or by a legally binding act of the European Union;

"**processing**" shall mean all processing operations carried out by a processor acting on behalf of or under the instructions of the controller;

"**transfer**" shall mean the making the data available to a specified third party;

"**disclosure**" shall mean making the data publicly available;

"**erasure**": shall mean rendering data unrecognizable in such a way that it is no longer possible to recover the data

"**profiling**" shall mean any processing of personal data by automated means intended to evaluate, analyze or predict personal aspects relating to the data subject, in particular their performance at work, economic situation, health, personal preferences or interests, reliability, behavior, location or movements;

5 Principles and basic provisions

5.1 Legality, fairness and transparency

The processing of personal data shall be lawful, fair and transparent for the Data Subject (Article 5 Section (1) paragraph (a) of the GDPR).

5.2 Goal orientation

Personal data may be collected only for specified, explicit and legitimate purposes, for the exercise of rights and the performance of obligations and may not be processed in a way incompatible with those purposes. Only personal data that is necessary for the purpose of the processing and adequate for the purpose for which it was collected may be processed. Personal data may only be processed to the extent and for the duration that is necessary for the intended purpose (Article 5 Section (1) paragraph (b) of the GDPR).

5.3 Data economy

The personal data must be adequate, relevant and limited to what is necessary for the purpose for which it is processed (Article 5 Section (1) paragraph (c) of the GDPR)

5.4 Accuracy

The personal data must be accurate and, where necessary, kept up to date; all reasonable steps must be taken to ensure that personal data that is inaccurate for the purpose of its procession is erased or rectified without delay (Article 5(1)(d) GDPR).

5.5 Limited storage

Personal data must be stored in a form which allows for the identification of Data Subjects for only as long as it is necessary for the purpose for which the personal data is processed; personal data may be stored for longer periods only if the personal data is processed in accordance with the applicable law for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organizational measures as provided for in this Regulation to safeguard the rights and freedoms of Data Subjects (Article 5 Section (1) paragraph (e) of the GDPR).

5.6 Integrity and confidentiality

The processing of personal data must be carried out in such a way as to ensure adequate security of personal data, including the protection against unauthorized or unlawful processing, accidental loss, destruction or damage, by using appropriate technical or organizational measures (Article 5 Section (1) paragraph (f) of the GDPR).

5.7 Accountability

The Data Controller is responsible for compliance with the data management principles and must be able to demonstrate such compliance (Article 5 Section (2) of the GDPR)

6 Ensuring data security

6.1 General Principles of Data Security:

The Data Controller and the data processor it uses shall implement appropriate technical and organizational measures to ensure a level of data security appropriate to the scale of the risk, taking into account the state of science and technology and the cost of implementation, the nature, scope, context and purposes of the processing, and the varying degrees of probability and severity of the risk of a possible security breach may pose to the rights and freedoms of natural persons concerned.

The Data Controller shall ensure the security of the personal data of the Data Subjects and shall implement the technical and organizational measures and establish the procedural rules necessary to enforce the GDPR, the Information Act and other data protection and confidentiality rules.

The Data Controller shall take appropriate measures to protect personal data against, in particular, unauthorized access, alteration, transmission, disclosure, erasure or destruction, accidental destruction or damage and inaccessibility resulting from changes in the technology used.

All persons involved in data management must exercise the utmost care in their work to ensure the authenticity and preservation of the data and to prevent unauthorized access.

Everyone person involved has access only to the data they need to do their job, and only to the extent they need it.

In order to protect the electronically processed data files in the different registers, the Data Controller shall ensure by appropriate technical means that the data stored in the registers cannot be directly linked and attributed to the Data Subject, unless permitted by law.

In order to maintain security and prevent processing in breach of the GDPR or the Info Act, the Controller shall assess the risks inherent in the nature of the processing and, where necessary, apply additional measures to mitigate those risks, such as encryption, pseudonymisation. Currently, the Controller does not apply such measures.

The Data Controller shall select and operate the IT tools used to process personal data in the course of providing its services in such a way that the personal data processed:

(a) is accessible to authorized persons only ("availability");

(b) authenticity and verification of the data ("authenticity of processing");

(c) can be verified ("data integrity");

(d) is protected against unauthorized access ("data confidentiality").

The Data Controller shall keep it during the processing:

(a) confidentiality: protect the Data Subject's personal data so that only those who are entitled to access it have access to it;

(b) integrity: it protects the accuracy and completeness of the information and the method of processing;

(c) availability: to ensure that when an authorised user acting on behalf of the Data Controller needs it, they have effective access to the information requested and the means to do so.

In order to enforce and ensure the conditions of data security, the Data Controller shall ensure the appropriate and regular training and further training of the employees, subcontractors and personal contributors concerned.

6.2 Main data security features and tools of the Data Controller's paper-based data management:

The Data Controller shall record the medical records on a medium of appropriate quality (traditional paper, form) after the patient transfer has been completed. The person recording the data shall be responsible for the legibility of the data.

The Data Controller shall ensure the storage and protection of paper documents containing personal data, in particular:

(a) protection against unauthorized access, including in particular the separate storage of documents containing personal data and ensuring that only authorized persons have access to them;

(b) the physical protection of documents, including in particular object protection measures, protection against fire, water damage, lightning, other elementary damage.

A paper document containing personal data may be forwarded to the Data Controller's partners (assistance service providers, insurance companies) only in a sealed envelope, if they request the provision of data on paper.

The Data Controller shall allocate access rights to documents containing personal data on an individual basis.

6.3 Main data security features and tools of the Data Controller's IT systems:

The IT service provider used by the Data Controller shall ensure the security of the IT system and the locking of the system components by means of administrative, physical and logical measures and protection procedures at system level, which shall consist of measures that can reasonably be expected in the state of the art and shall include in particular:

(a) protection against unauthorized access, including in particular strong password protection for access to systems and devices;

(b) measures to ensure the possibility of recovery of data files, in particular regular backups and the separate and secure management of such backups (copies);

(c) the protection of stored or otherwise managed data files against malicious codes and programs (virus protection, firewall, etc.);

(d) the physical protection of such data files or the media on which the data are stored, including in particular the protection of the object, the protection against

fire, water, lightning, other natural hazards and the recoverability of damage caused by such events.

The Data Controller also ensures the internal monitoring of its IT systems to ensure data security, during which any unusual use or other security deviations may be recorded. System monitoring also allows the effectiveness of the security measures in place to be checked.

The Data Controller shall allocate access rights to data files containing personal data on an individual basis.

Access to the computer equipment by an external person (e.g. maintenance) should preferably be ensured in such a way that the data processed are not made known to him/her.

6.3.1 Physical protection of the IT system

(i) General requirements

(a) IT equipment may only be used in a room with a security lock.

(b) The monitor must be positioned so that the data displayed cannot be read by unauthorized persons.

(c) The IT equipment may be used only by designated staff, and the user is responsible for its proper functioning and protection.

(ii) Hardware protection

(a) The equipment must be operated only in perfect condition and in accordance with its intended use.

(b) The necessary maintenance and servicing work must be carried out in accordance with the conditions provided for in the budget.

(c) Maintenance work should be carried out in a planned, careful and diligent manner. The organization of the work should take into account: the manufacturer's specifications, recommendations, experience, faults detected by hardware tests.

(d) The dismantling of the base machine should only be carried out by a professional.

(e) The computer system or any component of it may be changed only with the authorization of the administrator, and the time of replacement of any device must be documented.

(iii) Fire safety

(a) The general provisions on fire safety are set out in the Data Controller's Fire Safety Policy.

6.3.2 Personal protection of the IT system

(i) System software protection

(a) It is the responsibility of the administrator to develop, implement, monitor, evaluate and control the actions and measures to be taken by the Data Controller to ensure IT data security, and to grant and monitor individual access.

(b) The administrator ensures that the system software is kept up to date and that utilities and libraries are always available to users. Only the administrator may modify the system software, and a record of the changes must be kept.

(c) The use of real data for software development or testing should be avoided.

(ii) Protecting user programs

(a) Unauthorized access must be prevented when using the software.

(b) The administrator is responsible for the registration and maintenance of the programs.

(c) Only the administrator and developers can install any software on computers.

(d) An up-to-date register of the software must be kept, containing the following information: name of the system, software identifier, name of the software creator, copy number, date of delivery, name and date of modifications.

(iii) Protecting the recording of data

(a) The same person cannot record and check the same set of data.

(b) Data processing requires backups to be performed at specified intervals, in this case the administrator backs up the data to an external storage medium once every month.

(iv) Check

(a) Compliance with the provisions of the Code must be continuously monitored during the in-process inspection.

(b) The audit should help to prevent the emergence of existing IT system vulnerabilities. Once an emergency has occurred, the primary concern is to reduce damage and prevent recurrence.

6.3.3 Damage repair

In the event of an elemental disaster, the following shall be carried out immediately in the following order of priority when partial or total damage has occurred:

(a) the material that is still usable should be saved,

(b) from backups, backups of backups, backups of backups, the corrupted data must be restored,

(c) the creation of a room protected against damage,

(d) using archived material, processing should continue.

6.4 The Data Controller's basic internal data management practices in relation to the IT system for the Data Controller's colleagues:

All colleagues and collaborators of the Data Controller must comply with the following essential practices when processing personal data:

(a) In the course of the Data Controller's operations, only personal data that are indispensable for the process in question may be stored, transmitted and otherwise processed. The Data Controller's manager is responsible for the design of data and workflows accordingly (avoiding unnecessary data accumulation).

(b) When authorizing IT rights, it must be ensured that only those persons who have an indispensable need to have access to personal data for the purposes of their work are granted access to such data.

A document containing personal data sent by e-mail should only be sent as an attachment and in such a way as to ensure that it can only be viewed by the authorized person, by including - as a minimum - a warning sentence in the body of the e-mail, stating that "The *attachment to this e-mail contains personal data, which may only be viewed by the addressee.* "

A document containing personal data may be stored on shared drives used by the Data Controller (accessible by several employees, personal contributors, etc.) only if it is ensured that only authorized employees, personal contributors, etc. of the Data Controller can access it.

Employees and personal contributors of the Data Controller shall keep secure and protect the data media containing personal data that they use or have in their possession, regardless of the way in which the data are recorded, against unauthorized access, alteration, disclosure, disclosure, erasure or destruction, accidental destruction or damage.

7 Rights of Data Subjects and specific rights arising from healthcare

7.1 **Right of access** (Article 15 of the GDPR)

The Data Subject shall have the right to obtain from the Controller, upon request, information as to whether or not their personal data are being processed and, if such processing is ongoing, the right to access the personal data and the following information:

(a) the purposes of the processing;

(b) the categories of personal data;

(c) the recipients or categories of recipients to whom or with whom the personal data have been or will be disclosed by the Controller (in particular, recipients in third countries or international organizations);

(d) the envisaged duration of the storage of personal data and, where this is not possible, the criteria for determining that duration;

(e) the right to lodge a complaint with the National Authority for the Protection of Freedom of Information;

(f) and, where the data have not been collected directly from the Data Subject, any available information about their source.

The Data Controller shall inform the Data Subject of the measures taken in response to the request without undue delay, but not later than 30 (thirty) days from the receipt of the request.

If necessary, taking into account the complexity of the application and the number of applications, this deadline may be extended by a further 60 (sixty) days. The Data Controller shall inform the Data Subject of the extension of the time limit, stating the reasons for the delay, within 30 (thirty) days of receipt of the request. The information shall be provided to the Data Subject, where possible, by the means by which the request was made by the Data Subject, unless the Data Subject explicitly requests otherwise.

7.2 Right to rectification (Article 16 of the GDPR)

The Data Subject shall have the right to obtain from the Data Controller, upon their request and without undue delay, the rectification of inaccurate personal data relating to him or her and the completion of incomplete personal data.

7.3 Right to erasure (Article 17 of the GDPR)

The Data Subject shall have the right to obtain from the Controller, upon their request, the erasure of personal data relating to him or her without undue delay where one of the following grounds applies:

(a) the personal data are no longer necessary for the purposes for which they were collected or otherwise processed;

(b) the Data Subject withdraws their consent on the basis of which the processing is based, within the meaning of Article 6 Section (1) paragraph (a) or Article 9 Section (2) paragraph (a) of the GDPR, and there is no other legal basis for the processing;

(c) the Data Subject objects to the processing on the basis of Article 21 Section (1) GDPR and there are no overriding legitimate grounds for the processing, or the Data Subject objects to the processing on the basis of Article 21 Section (2) of the GDPR;

(d) the personal data have been unlawfully processed by the Controller;

(e) if the personal data must be deleted by law;

(f) the personal data have been collected in connection with the provision of information society services as referred to in Article 8 Section(1) of the GDPR (conditions for children's consent).

The Data Controller will not delete the processed data even if the Data Subject so requests, if the processing is still necessary for one of the following reasons:

(a) to exercise the right to freedom of expression and information;

(b) to comply with an obligation under the law that requires the processing of personal data;

(c) necessary for the establishment, exercise or defense of legal claims or interests.

In the above case, the Data Controller limits the processing of the Data Subject's personal data to the processing for the purposes set out above.

7.4 Right to restrict processing (Article 18 of the GDPR)

The Data Subject shall have the right to obtain, at their request, the restriction of processing by the Controller if any of the following conditions are met:

(a) the Data Subject contests the accuracy of the personal data, in which case the restriction applies for the period of time necessary to allow the Controller to verify the accuracy of the personal data;

(b) the processing is unlawful and the Data Subject opposes the erasure of the data and requests instead the restriction of their use;

(c) the Controller no longer needs the personal data for the purposes of processing, but the Data Subject requires them for the establishment, exercise or defense of legal claims; or

(d) the Data Subject has objected to the processing; in this case, the restriction applies for the period until it is established whether the legitimate grounds of the Controller prevail over the legitimate grounds of the Data Subject.

In case of restriction of processing, the personal data subject to the restriction may be processed, except for storage, only with the consent of the Data Subject or for the establishment, exercise or defense of legal claims or for the protection of the rights of another natural or legal person or for important public interests of the European Union or of a Member State.

The Data Controller shall inform the Data Subject requesting the lifting of the restriction in advance.

7.5 Right to data portability (Article 20 of the GDPR)

The Data Subject has the right to receive their personal data in a structured, commonly used, machine-readable format and the right to transmit such data to another controller without hindrance from that controller, provided that:

(a) the processing is based on consent within the meaning of Article 6 Section (1) paragraph (a) or Article 9 Section (2) paragraph (a) of the GDPR or on a contract within the meaning of Article 6 Section (1) paragraph (b) of the GDPR; and

(b) the processing is carried out by automated means.

The Data Controller **does not** currently processes data by automated means.

7.6 **Right to object** (Article 21 of the GDPR)

The Data Subject has the right to object at any time, on grounds relating to their particular situation, to the processing of their personal data based on Article 6(1)(e) or (f) of the GDPR, including possible profiling based on those provisions. In the event of a legitimate objection by the Data Subject, the Controller may no longer process the Data Subject's personal data unless the Data Subject demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the Data Subject or for the establishment, exercise or defense of legal claims.

7.7 **Specific rules on confidentiality**

As a Data Subject, the beneficiary is entitled to the protection of their personal data and the protection of the privacy of their private life. In the course of the air transport and care organization of the Data Controller, particular care shall be taken to ensure that only authorized persons have access to the Data Subject's data. The Data Controller shall also ensure that, in the course of air ambulance transport and care management, information relating to the health status and personal circumstances of the data subject is not disclosed to other Data Subjects or to unauthorized persons.

The patient concerned has the right to have their health and personal data disclosed by the persons involved in their healthcare only to the person entitled to receive them and to keep them confidential.

The Data Controller or any other person employed by or contracted to the Data Controller shall be bound by the obligation of confidentiality with regard to the personal data of the Data Subject, data concerning their health and other data that comes to their knowledge in connection with their employment, without any time limitation. The Data Controller shall be exempted from the obligation of confidentiality if the Data Subject or their legal representative has given their written consent to the transfer of the data within the limitations set out therein and the transfer of the data is required by law.

The patient concerned has the right to declare to whom information about their illness, its expected outcome may be disclosed and to whom partial or full access to their health data is excluded. The data subject's health data shall be disclosed without their consent if required by law or if necessary to protect the life, or health of others.

Without the consent of the patient concerned, health data, the lack of knowledge of which may lead to the deterioration of the patient's health, may be disclosed to the person providing further care and treatment of the patient.

The patient has the right to be examined and treated in the presence of only those persons whose participation is necessary for the treatment or those to whose presence the patient has consented, unless otherwise provided by law.

7.8 The right of access to medical records

The health record is held by the health care provider and the patient has the data in it. The Data Subject has the right to be informed about the processing of data in the context of their medical treatment, to be informed of the medical and personal data concerning him/her, to consult the medical records and to obtain copies thereof at their own expense. This right shall be exercised by a person authorized in writing by the Data Subject during the period of their care and by a person authorized by him/her in a private document with full probative value after the termination of their care.

In the event of the death of the Data Subject, their legal representative, close relative or heir shall be entitled, upon written request, to obtain access to medical data relating to the cause of death or to the treatment provided prior to the death, to consult the medical records and to obtain copies thereof at their own expense.

8 Rules for data processing

8.1 Informing the Data Subject about the processing

The Data Subject has the right to be informed about the processing of their personal data in a concise, transparent and easily accessible form, in a clear and comprehensible manner. The information relating to the processing of personal data concerning the Data Subject shall be provided to the Data Subject at the time of collection or, where the data have been collected from another source than the Data Subject, within a reasonable period of time having regard to the circumstances of the case.

Where personal data are collected from the Data Subject, the Data Subject must also be informed of the obligation to provide the personal data and of the consequences of not providing the data.

The Data Subject shall be informed of the fact of profiling and automated decision-making and its consequences. If personal data may lawfully be disclosed to another address, the Data Subject shall be informed of this at the time of the first disclosure to the address. If the Controller intends to process personal data for a purpose other than the purpose for which they were initially collected, the Data Subject must be informed of that other purpose and of any other necessary information before further processing.

If the Data Controller is unable to provide the Data Subject with information on the origin of the personal data because they originate from different sources, general information must be provided.

The information shall include (i) the identity and contact details of the Controller; (ii) the contact details of the Data Protection Officer of the Controller (if any); (iii) the purposes for which the personal data are intended to be processed and the legal basis for the processing; (iv) in the case of processing based on "legitimate interests", those legitimate

interests; (v) the recipients of the personal data; (vi) the envisaged duration of the processing; (vii) the right of the Data Subject to request the Controller to access, rectify, erase or restrict the processing of personal data relating to him or her and to object to the processing of such personal data, and the Data Subject's right to data portability; (viii) the right to lodge a complaint with a supervisory authority; (ix) whether the provision of the data is a prerequisite for the conclusion of a contract and the possible consequences of not providing the data; and (x) any automated decision-making, including profiling.

8.2 Lawfulness of processing

The processing of personal data is lawful if at least one of the following conditions are met:

(a) the Data Subject has given their consent to the processing of their personal data (Article 6 Section (1) paragraph (a) of the GDPR), or

(b) processing is necessary for the performance of a contract to which the Data Subject is a party or for the purposes of taking steps at the request of the Data Subject prior to entering into a contract (Article 6 Section (1) paragraph (b) of the GDPR); or

(c) processing is necessary for compliance with a legal obligation to which the controller is subject (Article 6 Section (1) paragraph (c) of the GDPR); or

(d) the processing is necessary for the protection of the vital interests of the Data Subject or of another natural person (Article 6(1)(d) of the GDPR); or

(e) the processing is necessary for the performance of a task carried out in the public interest (Article 6 Section (1) paragraph (e) of the GDPR), or

(f) the processing is necessary for the purposes of the legitimate interests pursued by the Controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require the protection of personal data, in particular where the Data Subject is a child (Article 6 Section (1) paragraph (f) of the GDPR)

9 Scope of personal data processed by the controller, purpose, legal basis and duration of each processing operation

9.1 Patient air transport

The Data Controller may process the personal identification data and health data of individuals (and their legal representative, named relatives) who request or actually use air patient transport (collectively) as Data Subjects necessary and sufficient for identification and air passenger transport for the following main purposes (Section 4 paragraph (1) of the Health Care Act):

(a) recording and assessing patient transport needs;

(b) providing patient transport care;

(c) promoting the preservation, improvement and maintenance of health;

(d) to promote effective medical treatment;

(e) monitoring the health of the Data Subject;

(f) taking measures necessary in the interests of public health, public health and epidemiology;

(g) the enforcement of patients' rights.

Scope of personal data processed	Legal basis for data processing	Purpose of data processing	Duration of data processing
• Full name; • Birth name; • Place and date of birth; • Mother's maiden name; • Address, place of residence; • Social security number (social security number); • Citizenship; • Details of the insurer/insurance company if care is financed by an insurer; • Medical history, medical history, results of tests and examinations used as a basis for diagnosis and treatment plan, date of tests, final reports; • Data on drug hypersensitivity; • Name and identification number of the doctor administering care.	Article 6 Section (1) paragraph (e) and Article 9 Section (2) paragraph(h) GDPR. According to Section 4 of the Eüak.tv.	Deciding, preparing and organizing the transportability of the patient concerned.	If the air transport of the Data Subject is not recommended, the data will be deleted on the sixtieth (60th) day the contact. Otherwise, the duration of data processing will be as follows.
• Full name; • Birth name; • Place and date of birth; • Mother's maiden name; • Address, place of residence; • Social security number (social security number); • Citizenship;	Article 6 Section (1) paragraph (c) and Article 9 Section (2) paragraph (h) of the GDPR. Based on Section 4 of the Eüak.tv. Pursuant to Section 27/A of the AT Act	Ensure the safe and appropriate air transport of the patient from abroad and their entry into the country of destination.	The medical documentation shall be kept for at least 30 (thirty) years from the date of data recording, and the final report for at least 50 (fifty) years (Section 30 paragraph(1) of the Health Care Act).By way of derogation, the

• Details of the insurer/insurance company if care is financed by an insurer; • In the case of a Data Subject with capacity to act, the name, address and contact details (telephone number or email address) of the person to be notified; • Name, address, contact details (telephone number or email address) of the legal representative in the case of a minor or a patient with partial or full incapacity; • Medical history, results of tests and examinations used as a basis for diagnosis and treatment plan, date of tests, final reports; • Data on drug hypersensitivity; • Name and identification number of the doctor administering care; • Travel document number, expiry date (copy of identity card or passport); • All other data and facts that may influence the patient's recovery.	Air travel ord. Section 8		record made by diagnostic imaging shall be kept for 10 (ten) years from the date of its making, and the report of the record shall be kept for 30 (thirty) years from the date of its making (Section 30 (2) of the Health Care Act).
• Full name; • Date of birth; • Travel document number, expiry date (copy of identity card or passport)	Article 6 Section (1) paragraph (e) of the GDPR. Pursuant to Section 27/A of the AT Act . Air travel ord. Section 8	Together with the Data Subject, ensure the proper and safe repatriation and entry into the country of destination of their relative and/or legal representative.	The general limitation period after the use of the service is 5 (five) years (Civil Code. Section 6:22 paragraph (1)).
• Full name; • Contact (phone or email)	Article 6 Section (1) paragraph(e) of the GDPR.	Maintaining contact with a relative of the Data Subject.	The general limitation period after the use of the service is 5 (five) years (Civil Code.

			Section 6:22 paragraph (1)).
• Full name of the doctor administering care; • Identification number; • Contact details (phone number and/or email address)	Article 6 Section (1) paragraph (e) of the GDPR.	Ensuring safe and appropriate air transport of the patient from abroad in accordance with the condition of the patient concerned.	The medical documentation shall be kept for at least 30 (thirty) years from the date of data recording, and the final report for at least 50 (fifty) years (Section 30 paragraph(1) of the Health Care Act).By way of derogation, the record made by diagnostic imaging shall be kept for 10 (ten) years from the date of its making, and the report of the record shall be kept for 30 (thirty) years from the date of its making (Section 30 (2) of the Health Care Act).

In the course of processing, the Data Controller may receive personal data relating to the Data Subject from third parties (such as insurers, assistance providers and relatives).

Pursuant to Article 28 of the Health Care Act, in order to transport the Data Subject to a hospital for further medical treatment, the Data Controller is obliged to order a ground patient transport service that meets the needs of the patient and to provide the Data Controller with information about the Data Subject and their condition, and to provide the medical documentation at the same time as the transport is provided.

The Data Controller uses a data processor for the flight organisation, to whom it transfers the data necessary for the journey and the entry into the country of destination.

The personal data of the Patient concerned are held on paper and in an electronic database.

Under the relevant provision of the Privacy Code, the Data Subject is required to provide credible proof of their personal data.

Health data and personal identification data (in relation to health) may also be processed for the purposes specified in Section 4 paragraph (2) of the Health Care Act, in cases specified by law.

Pursuant to the Health Care Act, health data may also be processed for purposes other than those set out above in this Policy, either in full or for specific processing activities, with the consent of the Data Subject or their legal or authorised representative, given

voluntarily and on the basis of appropriate information, clearly expressing their wishes and providing credible evidence that a lawful declaration has been made.

The retention of medical records beyond the time limit provided for in the Eüak.tv is possible if (i) they can be linked to other medical records of the Data Subject which are not older than 30 (thirty) years, and (ii) the nature of the disease, (iii) the nature of the treatment, (iv) the Data Subject, or (v) for reasons of general scientific and cultural history, they are of scientific significance.

The provision of health and personal identification data (in relation to health) by the Data Subject is voluntary, with the exception of the personal identification data required for the provision of health care and the data required under Article 13 of the Health Care Act.

In the event that the Data Subject voluntarily contacts the healthcare network, their consent to the processing of their health and personal data relating to the treatment shall be deemed to have been given, unless otherwise stated, and the Data Subject (legal representative or relative) shall be informed thereof. In cases of urgent necessity and where the Data Subject lacks capacity to consent, there shall be a presumption of voluntariness.

The Data Subject (legal representative, relative) is obliged to provide health and personal identification data to the Data Controller upon request of the patient care provider (Section 13 of the Health Care Act),

(a) if it is probable or confirmed that they are infected by a pathogen of a disease listed in Annex 1 of the Health Care Act, or suffers from poisoning of infectious origin or infectious disease, except in the case provided for in paragraph (6) of Article 15;

(b) if it is necessary to carry out the screening and aptitude tests listed in Annex 2 to the Health and Safety at Work Act;

(c) in case of acute poisoning;

(d) if it is probable that the Data Subject suffers from an occupational disease as defined in Annex 3 of the Health and Safety Act;

(e) if the provision of the data is necessary for the treatment, health care or protection of the health of the unborn child or minor child;

(f) if the competent authority has ordered the investigation for the purposes of law enforcement, crime prevention, prosecution, judicial proceedings or proceedings by the administrative authorities or the police;

(g) if the information is required for the purpose of verification under the National Security Services Act.

In the case of data processing and data handling pursuant to Section 4 (1) of the Eüak.tv., all health data relating to the illness of the data subject may be transmitted, which, according to the decision of the treating physician, is important for the treatment of the illness, unless the Data Subject prohibits this in writing or in a statement in the register of

self-determination. The Data Subject must be informed of this possibility before the transfer. In cases pursuant to Article 13 of the Eüak.tv., health and personal data shall be transmitted despite the Data Subject's objection.

Pursuant to Section 28 paragraph (3) of the Health Care Act, the Data Controller is obliged to prepare a so-called trasport report on the events during the treatment, which is forwarded to the insurance companies, assistance providers and hospitals that continue to treat the patient on behalf of the Data Subject. This document will form part of the medical record.

In case of urgent need, all medical and personal data known to the treating physician that may be related to the treatment may be transmitted.

9.2 Business travel

The Data Controller may process the personal identification data of individuals requesting and using business travel as Data Subjects necessary and sufficient for the identification and transportation by air of the Data Subjects on the basis of:

Scope of personal data processed	Legal basis for processing	Purpose of data processing	Duration of data processing
• Full name; • Email address; • Departure and destination; • Planned date; • Other travel information (number of passengers).	Article 6 Section (1) paragraph (a) of the GDPR.	Preparation of a quotation.	If the commercial relationship is not established, the data will be deleted on the 30th (thirtieth) day after the last contact.
• Full name; • Date of birth; • Travel document number, expiry date (copy of identity card or passport) • Address.	Article 6(1)(b) and (c) of the GDPR. Pursuant to Section 27/A of the AT act. Air travel ord. Section 8	Arranging flights and boarding in the country of destination for the Data Subjects in order to use their services.	The general limitation period after termination of the contract is 5 (five) years (Civil Code. Section 6:22 paragraph (1)). Pursuant to the Accounting Act, the data processed for the purpose of issuing and storing the voucher shall be processed for a period of 8 (eight) years after the termination of the contract (Section 169 paragraph (2) of the Accounting Act). Management and retention of accounting documents until the

			right to assess tax has expired, i.e. for 5 (five) years from the end of the year in which the return based on the document was filed (Taxation Act Section 47 paragraph (1) Section 164 paragraph (1)
• Full name; • Date of birth; • Address.	Article 6 Section (1) paragraph (f) of the GDPR.	Enforcement of the claims of the Data Controller arising from the above legal relationships (management of receivables, collection, enforcement of other claims)	Until the expiry of the general limitation period of 5 (five) years following the termination of the contract or, if a claim has been asserted by or against the Data Controller in relation to the Data Subject, the final adjudication of the claim (Civil Code. Section 6:22 paragraph (1)).

The Data Controller uses a data processor for the flight organisation, to whom it transfers the data necessary for the journey and the entry into the country of destination.

9.3 Cargo

The Data Controller may process the data of companies and their contact persons requesting and using cargo services as Data Subjects on the basis of the following:

Scope of personal data processed	Legal basis for data processing	Purpose of data processing	Duration of data processing
• Full name; • Email address; • Departure and destination; • Planned date; • Other travel information (details of products to be transported).	Article 6(1)(a) of the GDPR.	Preparation of a quotation.	If the commercial relationship is not established, the data will be deleted on the 30th (thirtieth) day after the last contact.
• Full name; • Address; • Phone number; • Tax number.	Article 6 Section (1) paragraph (b) of the GDPR.	Arranging necessary deliveries for the customer using the services of the Data Controller.	The general limitation period after termination of the contract is 5 (five) years (Civil Code. Section 6:22 paragraph (1)).

			Pursuant to the Accounting Act, the data processed for the purpose of issuing and storing the voucher shall be processed for a period of 8 (eight) years after the termination of the contract (Section 169 paragraph (2) of the Accounting Act). Management and retention of accounting documents until the last date of a valid assessment, that is 5 (five) years from the end of the year in which the tax return based on the document was filed (Taxation Act Section 47. paragraph (1) section 164. paragraph (1)
• Full name; • Address; • Phone number; • Tax number.	For the purposes of managing the above legal relationship pursuant to Article 6 Section (1) paragraph (f) of the GDPR.	Enforcement of the claims of the Data Controller arising from the above legal relationships (management of receivables, collection, enforcement of other claims)	Until the expiry of the general limitation period of 5 (five) years after the termination of the contract or, if a claim has been asserted by or against the Data Controller in relation to the Data Subject, the final adjudication of the claim (Civil Code Section 6:22 paragraph (1)).
• Full name; • Phone number; • Your electronic notification address (e-mail address); • Name of your employer.	Article 6 Section (1) paragraph (f) of the GDPR.	Relations with contractual and other partners in the course of the Data Controller's operations	Until the limitation period following the termination of the legal relationship, which is 5 (five) years (Civil Code Section. 6:22 paragraph (1)).

9.4 Patient care

The Data Controller may process the personal identification data and health data of individuals (or their legal representative, named relative) (collectively) who apply for or actually use the service as Data Subjects, which are necessary and sufficient for identification, for the following main purposes:

Scope of personal data processed	Legal basis for data processing	Purpose of data processing	Duration of data processing
• Full name; • Birth name; • Place and date of birth; • Mother's maiden name; • Address, place of residence; • Social security number; • Citizenship; • Details of the insurer/insurance company if the care service is financed by an insurer; • Medical history, results of tests and examinations used as a basis for diagnosis and as part of a treatment plan, date of tests, final reports; • Data on drug hypersensitivity; • Name and identification number of the doctor administering care; • All other data and facts that may influence the patient's recovery.	Article 6 Section (1) paragraph (e) and Article 9 Section (2) paragraph (h) of the GDPR. According to Section 4 of the Eüak. Act.	Organizing and preparing the care of the patient concerned.	If the air transport of the Data Subject is not recommended, the data will be deleted on the 30th (thirtieth) day after the contact. Otherwise, the duration of data processing will be as follows.
• Full name; • Birth name; • Place and date of birth; • Mother's maiden name; • Address, place of residence; • Social security number; • Citizenship; • Details of the insurer/insurance company if the care service is financed by an insurer;	Article 6 Section (1) paragraph (c) and Article 9 Section (2) paragraph (h) of the GDPR. Based on Section 4 of the Eüak. Act Pursuant to Section 27/A of the AT Act Eüak. ord Section 8	Ensure the safe and appropriate air transport of the patient concerned and their admission to the country of destination.	Medical documentation shall be kept for at least 30 (thirty) years from the date of data recording, and the final report shall be kept for at least 50 (fifty) years (Section 30 paragraph (1) of the Health Care Act).By way of derogation, the record made by diagnostic imaging shall be kept for 10 (ten) years from the date of its making,

• In the case of a Data Subject with capacity to act, the name, address and contact details (telephone number or email address) of the person to be notified; • Name, address, contact details (telephone number or email address) of the legal representative in the case of a minor or a patient with partial or full incapacity; • Medical history, results of tests and examinations used as a basis for diagnosis and treatment plan, date of tests, final reports; • Data on drug hypersensitivity; • Name and identification number of the doctor administering care; • Travel document (copy of identity card or passport); • All other data and facts that may influence the patient's recovery.			and the report of the record shall be kept for 30 (thirty) years from the date of its making (Section 30 paragrap (2) of the Health Care Act).
• Full name; • Date of birth; • Travel document (copy of identity card or passport)	Article 6 Section (1) paragraph (e) of the GDPR. Pursuant to Section 27/A of the AT Act Eüak. ord Section 8	Together with the Data Subject, ensure the proper and safe air transportation and boarding of their relative and/or legal representative to the country of destination.	The general limitation period after the use of the service is 5 (five) years (Civil Code. Section 6:22 (1)).
• Full name; • Contact (phone or email)	Article 6 Section (1) paragraph (e) of the GDPR.	Maintaining contact with a relative of the Data Subject.	The general limitation period after the use of the service is 5 (five) years (Civil Code. Section 6:22 paragraph (1)).

In other respects, the processing of your data in the course of the provision of care is also governed by the provisions detailed in section 9.1 of this Policy.

9.5 Health education

The Data Controller may process the personal identification data of individuals requesting and receiving health education as Data Subjects that are necessary and sufficient for the identification of the Data Subjects on the basis of:

Scope of personal data processed	Legal basis for data processing	Purpose of data processing	Duration of data processing
• Full name; • Phone number; • Your electronic notification address (e-mail address); • Name of your employer.	Article 6 Section (1) paragraph (f) of the GDPR.	Relations with contractual and other partners in the course of the Data Controller's operations	Until the limitation period following the termination of the legal relationship, which is 5 (five) years (Civil Code Section. 6:22 paragraph (1)).
• Full name; • Address; • Phone number; • Tax number.	In order to provide a service to the Data Subject or the Controller pursuant to Article 6 Section (1) paragraph (b) GDPR.	In relation to the contract for the provision of services by or to the Data Controller, to maintain contact, issue and keep records in accordance with the Accounting Act.	If the commercial relationship is not established, the data will be deleted on the 30th (thirtieth) day after the last contact. The general limitation period after the termination of the contract is 5 (five) years (Civil Code. Section 6:22 paragraph (1)). In respect of the data processed for the purpose of issuing and retaining the voucher pursuant to the Accounting Act, the data processing period is not 8 (eight) years after the termination of the contract (Section 169 paragraph (2) of the Accounting Act). Accounting vouchers are processed and retained until the right to tax assessment has expired, i.e. 5 (five) years after the end of the year in which the tax return based on the voucher was filed (Taxation Act Article 47 (1), Article 164 (1))

• Full name; • Address; • Phone number; • Tax number.	For the purposes of managing the above legal relationship pursuant to Article 6(1)(f) GDPR.	Enforcement of the claims of the Data Controller arising from the above legal relationships (management of receivables, collection, enforcement of other claims)	Until the expiry of the general limitation period of 5 (five) years after the termination of the contract or, if a claim has been asserted by or against the Data Controller in relation to the Data Subject, the final adjudication of the claim (Civil Code. 6:22 (1)).

9.6 Advising Services

The Data Controller may process the personal identification data of the individuals requesting and using the counselling services as Data Subjects, which are necessary and sufficient for the identification of the Data Subjects, on the basis of:

Scope of personal data processed	Legal basis for data processing	Purpose of data processing	Duration of data processing
• Full name; • Phone number; • Your electronic notification address (email address); • Name of your employer.	Article 6 Section (1) paragraph (f) of the GDPR.	Relations with contractual and other partners in the course of the Data Controller's operations	Until the limitation period following the termination of the legal relationship, which is 5 (five) years (Civil Code Section. 6:22 paragraph (1)).
• Full name; • Address; • Phone number; • Tax number.	In order to provide a service to the Data Subject or the Controller pursuant to Article 6 Section (1) paragrapj (b) GDPR.	In relation to the contract for the provision of services by or to the Data Controller, to maintain contact, issue and keep records in accordance with the Accounting Act.	If the commercial relationship is not established, the data will be deleted on the 30th (thirtieth) day after the last contact.The general limitation period after the termination of the contract is 5 (five) years (Civil Code. Section 6:22 paragraph (1)). In respect of the data processed for the purpose of issuing and retaining the voucher pursuant to the Accounting Act, the data processing period is not 8 (eight) years after the termination of the contract (Section

			169 paragraph (2) of the Accounting Act). Accounting vouchers are processed and retained until the right to tax assessment has expired, i.e. 5 (five) years after the end of the year in which the tax return based on the voucher was filed (Taxation Act Section 47 paragraph, Section 164 paragraph(1))
• Full name; • Address; • Phone number; • Tax number.	For the purposes of managing the above legal relationship pursuant to Article 6 Section (1) paragraph (f) GDPR.	Enforcement of the claims of the Data Controller arising from the above legal relationships (management of receivables, collection, enforcement of other claims)	Until the expiry of the general limitation period of 5 (five) years after the termination of the contract or, if a claim has been asserted by or against the Data Controller in relation to the Data Subject, the final adjudication of the claim (Civil Code. Section 6:22 paragraph (1)).

9.7 Processing of personal data relating to employees

The Data Controller shall process the personal data of individuals who are employed by it or wish to enter into such a legal relationship in accordance with the Employer's Data Processing Policy and Information Notice, which is Annex 1 to this Policy.

9.8 Processing of personal data relating to personal contributors

The Data Controller shall process the personal data of individuals who have a personal contributor relationship with the Data Controller or who wish to establish such a relationship in accordance with the Personal Data Management Policy and Information Notice for Personal Contributors, which is set out in Annex 2 to this Policy.

9.9 Processing of personal data relating to agents, contractors

The Data Controller shall process the personal data of individuals who are in a relationship with it as a principal or contractor or wish to establish such a relationship in accordance with the Principal and Contractor Data Processing Policy and Information Notice, which is Annex 3. to these Policy.

9.10 Data processing on the website of the Data Controller

9.10.1 Use of cookies

The Data Controller **does not use** cookies on the website (https://www.trustair.hu/) to personalize the services of the website and improve its quality.

9.10.2 Contact

Through the website of the Data Controller, Data Subjects can contact the Data Controller if they have any questions about the service. The Controller may process the data provided by the Data Subject for the following main purposes:

Scope of personal data processed	Legal basis for processing	Purpose of data processing	Duration of data processing
• Full name; • Electronic notification address (email address)	Article 6 Section (1) paragraph (a) of the GDPR.	To answer a question or provide other information requested by the Data Subject.	The data will be deleted until the consent is withdrawn, but no later than on the 30th (thirtieth) day after the last contact.

9.10.3 Request for quotation

Through the Data Controller's website, Data Subjects can request an offer of the Data Controller's services. The Data Controller may process the data provided by the Data Subject for the following main purposes:

Scope of personal data processed	Legal basis for processing	Purpose of data processing	Duration of data processing
• Full name; • Email address; • Departure and destination; • Planned date; • Other travel information (number of passengers, patient transport details, etc.).	Article 6 Section (1) paragraph (a) of the GDPR.	Preparation of a price quotate.	If the commercial relationship is not established, the data will be deleted on the 30th (thirtieth) day after the last contact.the last contact.

9.11 Data processing on the Controller's Facebook, Instagram and LinkedIn pages

The Facebook page, https://www.facebook.com/, is operated by Facebook Inc. (1601 S. California Ave, Palo Alto, CA 94304, USA), which is the responsibility of Facebook Ireland Limited (Hanover Reach, 5-7 Hanover Quay, Dublin 2, Ireland) in Europe. Plugins are usually marked with the Facebook logo.

The Instagram page, https://www.instagram.com/, is operated by Facebook Inc. (1601 S. California Ave, Palo Alto, CA 94304, USA), which is the responsibility of Facebook Ireland Limited (Hanover Reach, 5-7 Hanover Quay, Dublin 2, Ireland) in Europe. Plugins are usually marked with the Instagram logo.

LinkedIn's website, https://www.linkedin.com/, is operated by LinkedIn Ireland Unlimited Company, Wilton Place, Dublin 2, Ireland. Plugins are usually marked with the LinkedIn logo.

The Data Controller has no control over the nature and extent of the data collected by social networks and only transfers to Facebook, Instagram and LinkedIn the data that may be collected and processed by the Facebook, Instagram and LinkedIn plug-in used by the Website at any time, provided that the Data Subject gives their explicit consent as described above or uses the Facebook, Instagram and LinkedIn plug-in.

Facebook and Instagram social networking service providers, in accordance with their respective practices and policies, store the data collected about the data subject as a user profile and use it for the purposes of advertising, market research and/or demand-oriented website design. In particular, such assessment is made in order to develop demand-led advertising (including to non-logged-in users) and to inform other users of the social network about the activities of the Data Subject on the website. The data subject has the right to object to the creation of these user profiles, in which case he/she should contact the provider of the plug-in in question in order to exercise this right.

It is important to note that the data collected in connection with browsing as described above will be transmitted regardless of whether the Data Subject has an account with the plug-in provider and is logged in.

LinkedIn provides anonymized statistical data on users and visitors to the LinkedIn page of the Data Controller for the company profile. These so-called "Profile-Insights" statistics are aggregated statistics that are generated by certain activities and recorded by LinkedIn when users and visitors interact with the Controller's corporate profile and related content.

For more information about the purpose and scope of data collection and processing by Facebook, Instagram and LinkedIn, please refer to the respective privacy policies of Facebook, Instagram and LinkedIn, where you can find further information about your rights and the options available to you to protect your data.

10 Records of processing activities

The Data Controller and its representative (Data Protection Officer) **shall keep** a register of the processing activities under its responsibility with regard to the provisions of Article 30 of the GDPR.

11 Data protection impact assessment

With regard to the impact of the envisaged processing operations on the protection of personal data, the Controller shall carry out an impact assessment prior to the start of the processing where the type of processing envisaged, in particular using new technologies, is likely to present a high risk to the rights and freedoms of natural persons, taking into account its nature, scope, context and purposes. If, on the basis of the risk assessment carried out, the envisaged processing is likely to significantly affect the exercise of a fundamental right of the Data Subjects, the Controller shall, except in cases of mandatory processing, prior to the start of the processing, provide a written analysis of the likely effects of the envisaged processing on the exercise of the fundamental rights of the Data Subjects, which shall also include the measures envisaged to address the risks and the measures taken by the Controller to ensure the exercise of the right to personal data.

12 Data retention and deletion

The Data Controller may store the Data Subject's personal data only for the shortest possible period of time. This period shall be determined taking into account the reason for the processing and the legal requirements applicable to the Controller to keep the data for a specified period (e.g. legislation requiring the retention of health data for a specified period).

The Controller shall delete the personal data if:

(a) its processing is unlawful;

(b) the Data Subject requests it in accordance with Section 7.3 of this Policy, and none of the cases listed and specified in the exceptions apply;

(c) the data is incomplete or inaccurate - and this situation cannot be lawfully remedied - provided that deletion is not excluded by law;

(d) the purpose of the processing has ceased or the statutory time limit for storing the data has expired;

(e) ordered by a court or the National Authority for Data Protection and Freedom of Information;

(f) the erasure of the data is required by law.

The Data Controller may process personal data that constitute banking secrecy in relation to an unconcluded service contract for as long as a claim can be made in relation to the failure of the contract, after which they must be deleted. The Data Controller may process customer data and personal data that constitute banking secrecy in relation to an unconcluded service contract for as long as a claim can be made in relation to the failure of the contract. Unless otherwise provided by law, the general limitation period laid down in the Civil Code shall apply.

In the event of deletion, the Data Controller shall render the data unidentifiable. Where required by law, the Controller shall destroy the storage medium containing the personal data. The Data Controller reserves the right to keep the deleted data in an unidentifiable form.

Erroneous health data cannot be deleted after the data has been recorded, but must be corrected so that the data originally recorded can be identified.

13 Data transfer

Within the Data Controller's organization, the personal data of the Data Subjects may only be transferred in accordance with the purpose limitation principle and access to such data may only be granted for an appropriate purpose.

The Controller may use the Data Subjects' personal data for direct marketing, direct marketing or information purposes, in particular for its own commercial purposes, only with the Data Subject's explicit and prior consent.

13.1 General rules for data transfers to third parties outside the Data Controller

Personal data may be transferred to third parties only on the basis of a legal authorization or with the prior consent of the Data Subject.

Prior to the transfer, the Data Controller is obliged to check whether the legal conditions for the transfer are met and whether the conditions for the processing of each personal data are met after the transfer.

The Data Protection Officer must be involved in the examination of the lawfulness of the transfer before the transfer is made to the same controllers for the same Data Subject and for the same purpose. Subsequent transfers do not require a separate assessment.

13.1.1 Personal data relating to health services may be transferred under the Eüakt Act as follows:

Pursuant to Section 28 paragraph (1) of the Eüakt Act, the health and personal data recorded about the Data Subject, necessary for the purposes of medical treatment, and their transmission must be recorded. The record of the data transfer must include the recipient of the data transfer, the manner and time of the transfer and the scope of the data transferred. The means of recording may be any data storage device or method that ensures the protection of the data as required by law. The treating physician shall keep a record of the medical data recorded by him or by the other care provider and of his own activities and actions in relation thereto. The record shall form part of the register.

- personal data relating to the healthcare service may be transferred to the healthcare providers receiving the treatment of the Data Subject for the purpose of facilitating the treatment;
- to the office of the Chief Medical Officer at the National Sanitary and Health Service Authority (ÁNTSZ), for the purpose of carrying out administrative activities related to health services

13.2 Transfers abroad or to a third country

Prior to the transfer, the Data Controller, with the involvement of the Data Protection Officer, is obliged to verify that the legal conditions for the transfer are met and that the conditions for the processing are met for each personal data subject to the transfer.

The Data Controller confirms, pursuant to Article 13 Section (1) paragraph (f) of the GDPR, that at the date of entry into force of this Policy, it will not transfer any data processed by it to an international organisation.

The Controller, pursuant to Article 13 Section (1) paragraph (f) of the GDPR, confirms that, at the time of the entry into force of this Policy, in the case of air transportation to a third country of a person cared for by the Controller or to another country for the purpose of organising care, the Controller will only transfer personal data to the air or ground ambulance service or to a relative of the controller, as set out in this Policy, if at least one of the following conditions is met:

- the Data Subject has given their explicit consent to the envisaged transfer after having been informed of the potential risks of the transfer due to the lack of a conformity decision and appropriate safeguards;
- the transfer is necessary for the performance of a contract between the Data Subject and the Data Controller or for the implementation of pre-contractual measures taken at the request of the Data Subject;
- the transfer is necessary to protect the vital interests of the Data Subject or of another person and the Data Subject is physically or legally incapable of giving consent.

In other cases, the Data Controller will not transfer data it processes to third countries.

13.3 Provision of data following a request from a public authority

On the basis of a request for data from official bodies (in particular, but not limited to, courts, prosecutors' offices, investigating authorities, law enforcement authorities, administrative authorities, the National Authority for Data Protection and Freedom of Information, or other bodies authorized by law), the Data Controller shall provide information, disclose data, transfer data or make documents available in the manner and with the content specified therein, if the request for data from the requesting authority is, to the best of the Data Controller's knowledge, likely to be lawful. The Controller excludes any further liability for any unlawfulness of the transfer of personal data to official bodies.

13.4 Personal data processed by the Data Controller may be transferred without the consent of the Data Subject:

(a) to bodies (conciliation bodies, supervisory authorities, etc.) entitled by law to settle any disputes between the Data Controller and the Data Subject;

(b) if the Data Subject is unable to give their consent for reasons beyond their control, in order to protect the vital interests of the Data Subject or of another person, or to prevent or counter a threat to the life, physical integrity or property

of a person, to the authorized body, upon request by a body authorized to access the data by a specific law;

(c) to legal representatives (law firms) involved in the enforcement of the Data Controller's rights;

(d) in the event of (sub)assignment by the Data Controller to third parties of a claim against the Data Subject or a company represented/owned by the Data Controller, the data concerning the claims concerned and the debtors of the claims to the assignee or the person making an offer for the claim;

(e) by the Data Controller to any other administrative body, authority, court, bailiff who is (are) conducting any legal proceedings necessary for the recovery of the claim in order to enforce the claim against the Data Subject or the company represented/owned by the Data Subject;

(f) to other public authorities to which the provision of information is required by the legislation in force, in the manner and to the extent provided for by such legislation;

(g) other persons or organizations who, on behalf of the Data Controller, are otherwise involved as processors in the preparation or performance of a contractual relationship between the Data Subject and the Data Controller.

14 Data processors

14.1 General rules for Data Processors

The Data Controller may, in the course of its operations, use a data processor to whom it transfers some or all of the Data Subject's personal data in order to provide services to the Data Subjects.

The processor may use an additional processor. The Processor shall inform the Data Controller of the additional processor used.

The Data Controller informs the Data Subjects that the persons entitled to process the data are those for whose performance of their tasks the knowledge of the personal data is indispensable.

The Data Controller shall update this Policy in any case of a change in the identity of the data processor. The processor may use an additional processor. The Data Controller shall be informed by the Processor of the additional processor used and the Data Controller shall subsequently indicate the identity of the additional processor in this Policy.

14.2 Processors used by the Data Controller

Data processor: **AXA Global Healthcare International House**
Data processing activity: insurance, assistance services
E-mail: AGHComplianceReporting@axa.com
Processing technology: computer program

Data subject of the processing: all personal data processed on servers and computer equipment.

Data processor: **Allianz Global Investors GmbH**
Data processing activity: insurance, assistance service provider
E-mail: privacy@allianzgi.com
Processing technology: computer program
Data subject of the processing: all personal data processed on servers and computer equipment.

Data processor: **Europ Assistance Hungary Kft.**
Data processing activity: insurance, assistance service provider
E-mail: dpo@europ-assistance.hu; EAGlobalDPO@europ-assistance.com;
Processing technology: computer program
Data subject of the processing: all personal data processed on the server, computer equipment.

Data processor: **Euro-Center Holding SE**
Data processing activity: insurance, assistance services
Telephone number: +420 221 860 330
Processing technology: computer program
Data subject of the processing: all personal data processed on servers and computer equipment.

Data processor: **AIG Europe S.A.**
Data processing activity: insurance, assistance services
E-mail: reception.hu@aig.com
Processing technology: computer program
Data subject of the processing: all personal data processed on servers and computer equipment.

Data processor: **Österreichischer Automobil-, Motorrad- und Touring Club (ÖAMTC)**
Data processing activity: insurance, assistance services
E-mail: datenschutz@oeamtc.at
Processing technology: computer program
Data subject of the processing: all personal data processed on servers and computer equipment.

Data processor: **Aeroplan Privacy Office**
Data processing activity: flight loyalty programme
E-mail: AeroplanPrivacy@aircanada.ca
Processing technology: computer program
Data subject of the processing: all personal data processed on servers and computer equipment.

Data processor: **air ambulance and air ambulance association SkyCU**
Data processing activity: air transport services for its members

E-mail: dpo@skycu.org
Processing technology: computer program
Data subject of the processing: all personal data processed on servers and computer equipment.

Data processor: **Air Bohemia a.s.**
Data processing activity: flight scheduling
E-mail: sales@airbohemia.cz
Processing technology: computer program
Data subject of the data processing: all personal data processed on servers and computer equipment.

Data processor: **Szántó András Gábor EV.**
Data processing activity: accounting
E-mail: smallbusiness@t-online.hu
Processing technology: computer program
Data subject of the processing: all personal data processed on servers and computer equipment.

Data processor: **Róbert Tibor Tofán**
Data processing activity: IT specialist
E-mail: trustair.admin@trustair.hu
Processing technology: computer program
Data subject of the processing: all personal data processed on servers and computer equipment.

Data processor: **ground ambulance services**
Data processing activity: transport of the data subject to an appropriate hospital.

15 Data protection incident

A data breach is a breach of security within the meaning of the GDPR that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Any employee, processor or other person involved in the processing of personal data who becomes aware of a personal data breach shall notify the Data Controller without delay to the Data Controller's representative or the Data Protection Officer, who shall promptly investigate and propose the necessary measures and ensure and monitor the implementation of the measures set out below.

15.1 Reporting a data protection incident

The Data Controller shall notify the data protection incident to the competent supervisory authority (NAIH) without undue delay and, if possible, no later than 72 hours after becoming aware of the data protection incident, unless the data protection incident is unlikely to pose a risk to the rights and freedoms of natural persons. If the notification is not made within 72 hours, it must be accompanied by the reasons justifying the delay.

The information to be provided must include

- the nature of the incident, including, where possible, the categories and approximate number of Data Subjects and the categories and approximate number of data subjects affected by the incident;
- the name and contact details of the Data Controller's representative or Data Protection Officer as contact person;
- the likely consequences of the incident;
- the measures taken or envisaged by the Data Controller to remedy the personal data breach, including, where applicable, measures to mitigate any adverse consequences of the personal data breach.

15.2 Information for Stakeholders

Where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the representative of the Data Controller shall, without undue delay, inform the Data Subject of the personal data breach, indicating its nature, the name and contact details of the Data Controller's contact person, the likely consequences and the measures taken or envisaged to remedy or mitigate the personal data breach, unless one of the cases provided for in Article 34(3) of the GDPR applies.

15.3 Data breach investigation, handling

The person in charge of the process that handles or processes the data must inform the Data Controller's representative or the Data Protection Officer of the measures taken to remedy the data breach immediately after the implementation of the measures in question, but no later than within 2 (two) working days.

15.4 Records of data protection incidents

The Data Controller shall keep a record of the data breach, which shall include the facts relating to the data breach, its effects and the measures taken to remedy it.

16 Data Protection Officer

With regard to Article 37 Section (1c) of the GDPR, the Data Controller has appointed a Data Protection Officer, whose name and contact details are set out in section 2.3 of this Policy.

The Data Protection Officer of the Controller shall perform the tasks assigned to him/her in the GDPR, including:

- provide information and professional advice to the Data Controller and its staff carrying out processing in relation to their obligations under the GDPR and other EU or Member State data protection provisions;
- monitor compliance with the GDPR and other EU or Member State data protection provisions and the Controller's or processor's internal rules on the protection of personal data, including the assignment of responsibilities, awareness raising and training of staff involved in data processing operations, and related audits;

- on request, provide technical advice on the data protection impact assessment and monitor the conduct of the impact assessment;
- cooperate with the supervisory authority; and
- act as a contact point for the supervisory authority on matters relating to data management and consult it on any other matter as appropriate.

17 Complaints and redress

The Data Subject may take the Data Controller to court in the event of a breach of their rights. The court shall rule on the case out of turn. The Data Controller shall prove that the processing complies with the law. The court of law, in the capital city the Metropolitan Court, has jurisdiction to decide the case. The action may also be brought before the court of the place of residence or domicile of the Data Subject.

The Data Controller shall compensate for any damage caused to others by unlawful processing of the Data Subject's data or by breaching the requirements of data security. The Controller shall be exempted from liability if it proves that the damage was caused by an unavoidable cause outside the scope of the processing. No compensation shall be due in so far as the damage resulted from the intentional or grossly negligent conduct of the injured party.

The Data Subject may also contact the National Authority for Data Protection and Freedom of Information in the event of a complaint regarding the processing of their personal data (Dr. Attila Péterfalvi, President of the National Authority for Data Protection and Freedom of Information, postal address: 1363 Budapest, PO Box 9, address: 1055 Budapest, Falk Miksa Street 9-11; telephone: +36 (1) 391-1400; fax: +36 (1) 391-1410; e-mail: ugyfelszolgalat@naih.hu; website: www.naih.hu).

18 Final provisions

This Policy may be amended by the representative of the Data Controller as provided by law.

The representative of the Data Controller undertakes to review the Rules and Regulations pursuant to Section 3 paragraph (3) of the Eüak. ord. as necessary, but at least every 3 (three) years.

With the entry into force of this Policy, the previous Privacy and Data Security Policy is repealed.

19 Annexes

1. Annex No.1: Employer's Data Management Policy and Information Notice
2. Annex 1: Personal Data Management Policy and Information Notice
3. Annex 1: Principal, Contractor Privacy Policy and Information Notice