D R A F T

Code of Conduct concerning personal data protection of **Travel Service, a.s.**, registered office Praha 6, K Letišti 1068/30, postal code: 168 00, ID: 25663135, and in the companies engaged in civil air transport, the controlling entity of which is Travel Service, a.s., namely:

Travel Service, a.s., registered office Praha 6, K Letišti 1068/30, 160 08, CZ
Travel Service Slovensko s.r.o., registered office Ivanská cesta 30/B, Bratislava 821 04, SK
Travel Service Kft., registered office Wesselényi u. 16/A, Budapest, 1077, HU
Travel Service Polska, Sp. z o.o., registered office ul. Gordona Bennetta 2B, Warszawa, 02-159, PL
Travel Service Gmbh, registered office Theatinerstraße 23, 80333 München, DE

and other companies declaring that they accede to this Code

hereinafter referred to as the

"**CODE**"

VERSION: 1.0

Valid: from 1 November 2018

I.
INTRODUCTION

Civil aviation is a specific field covering various spheres, especially the sphere of personal data protection. When performing this activity, data controllers collect a large quantity of various personal data they process and provide to other recipients even in third countries. The objective of this document is to increase the airline passengers' awareness of the processing of their personal data and to strengthen their confidence in legitimate processing of such

personal data as well as to provide guidance to those airlines which declare that they accede to this Code.

II.
Relevant Normative Legal Acts

The rights and obligations in civil aviation are regulated by a large number of regulations, orders, directives and decisions of the EU Commission or the executive director of EASA. These regulations also set out the conditions of processing the personal data of passengers, in many respects even more strictly than the conditions set out in General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council (hereinafter referred to as "GDPR").

The aforesaid regulations are, in particular:

- Act No 49/1997 of the Collection of Laws of the Czech Republic (Sb.), on civil aviation (for CZ)
- Act No 181/2014 Sb., on cybernetic security (for CZ)
- Decree No 466/2006 Sb., on the flight safety standard (for CZ)
- Regulation (EC) No 216/2008 of the European Parliament and of the Council of 20 February 2008 on common rules in the field of civil aviation and establishing a European Aviation Safety Agency, and repealing Council Directive 91/670 EEC, Regulation (EC) No 1592/2002 and Directive 2004/36/EC
- Regulation (EU) No 376/2014 of the European Parliament and of the Council on the reporting of occurrences in civil aviation
- Regulation (EC) No 1107/2006 concerning the rights of disabled persons and persons with reduced mobility when travelling by air
- Commission Regulation (EU) No 748/2012 of 3 August 2012 laying down implementing rules for the airworthiness and environmental certification of aircraft and related products, parts and appliances, as well as for the certification of design and production organisations

- Commission Regulation (EU) No 1321/2014 of 26 November 2014 on the continuing airworthiness of aircraft and aeronautical products, parts and appliances, and on the approval of organisations and personnel involved in these tasks
- Commission Regulation (EU) No 965/2012 of 5 October 2012 laying down technical requirements and administrative procedures related to air operations pursuant to Regulation (EC) No 216/2008 of the European Parliament and of the Council
- Commission Regulation (EU) 2015/640 of 23 April 2015 on additional airworthiness specifications for a given type of operations and amending Regulation (EU) No 965/2012
- Commission Regulation (EU) No 1178/2011 of 3 November 2011 laying down technical requirements and administrative procedures related to civil aviation aircrew pursuant to Regulation (EC) No 216/2008 of the European Parliament and of the Council
- Commission Regulation (EU) No. 1332/2011 of 16 December 2011 laying down common airspace usage requirements and operating procedures for airborne collision avoidance
- Commission Implementing Regulation (EU) No. 923/2012 of 26 September 2012 laying down the common rules of the air and operational provisions regarding services and procedures in air navigation and amending Implementing Regulation (EU) No 1035/2011 and Regulations (EC) No 1265/2007, (EC) No 1794/2006, (EC) No 730/2006, (EC) No 1033/2006 and (EU) No 255/2010 (Text with EEA relevance)
- Commission Implementing Regulation (EU) No 1034/2011 of 17 October 2011 on safety oversight in air traffic management (ATM) and air navigation services and amending Regulation (EU) No 691/2010
- Commission Implementing Regulation (EU) No 1035/2011 of 17 October 2011 laying down common requirements for the provision of air navigation services and amending Regulations (EC) No 482/2008 and (EU) No 691/2010.

- Commission Regulation (EU) 2015/340 of 20 February 2015 laying down technical requirements and administrative procedures relating to air traffic controllers' licences and certificates pursuant to Regulation (EC) No 216/2008 of the European Parliament and of the Council, amending Commission Implementing Regulation (EU) No 923/2012 and repealing Commission Regulation (EU) No 805/2011
- Commission Implementing Regulation (EU) 2017/373 of 1 March 2017 laying down common requirements for providers of air traffic management/air navigation services and other air traffic management network functions and their oversight, repealing Regulation (EC) No 482/2008, Implementing Regulations (EU) No 1034/2011, (EU) No 1035/2011 and (EU) 2016/1377 and amending Regulation (EU) No 677/2011
- Commission Regulation (EU) No 139/2014 of 12 February 2014 laying down requirements and administrative procedures related to aerodromes pursuant to Regulation (EC) No 216/2008 of the European Parliament and of the Council
- Commission Regulation (EU) No 452/2014 of 29 April 2014 laying down technical requirements and administrative procedures related to air operations of third country operators pursuant to Regulation (EC) No 216/2008 of the European Parliament and of the Council
- Directive (EU) 2016/681 of the European Parliament and of the Council on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime
- Commission Decision on standard contractual clauses for the transfer of personal data to third countries, including amendments
- Agreement between the EU and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service
- Agreement between the EC and the Government of Canada on the processing of Advance Passenger Information and Passenger Name Record data
- Agreement between the USA and the EU on the use and transfer of passenger name records to the United States Department of Homeland Security

- Bilateral aviation agreements that secure the right to personal data exchange, based on the reciprocal right of an airline to select a check-in agent for the territory of the other state party.
- Multilateral agreements concerning civil air transport
- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe, ETS 108, 1981, hereinafter referred to as "Convention No. 108"), ratified by the states the up-to-date and full list of which is available here: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures
- Commission Decisions on the adequate level of personal data protection provided by the Faeroese Act, in Jersey, in the Isle of Man, in Guernsey, Argentina, Switzerland, Israel, Eastern Republic of Uruguay, Principality of Andorra and New Zealand.

III.
Purpose

The purpose of this Code is to set out the general principles of the collecting and processing of personal data for service providers in the field of civil aviation, which will become binding on the service providers if they declare that they accede to this Code. Based on this Code, the providers will provide passengers with clear, comprehensible and transparent information as to how their personal data will be used, so as to facilitate their informed decision-making before the air transport. This information will help to secure that the data are used in a fair and transparent manner and that passengers travel with confidence in correct processing of their personal data. The ambition of the Code is to explain to the data subjects the context of processing and the necessity to transfer their personal data to other recipients and processors of personal data even into third countries. The objective of this document is to facilitate personal data protection by air transport providers through the support of time-proven procedures, their monitoring and unification of procedures at joint meetings of acceding members. The recommendations described in this document are targeted at the service providers in the field of civil aviation in the Czech Republic and, as the case may be, other

providers established in the EU if such providers not only accede to this document but also incorporate any national deviations into their internal binding rules. This document may become a part of corporate rules if so decided by individual data controllers.

The requirement of this Code is its pragmatism and the broadest generality possible; therefore, this Code cannot substitute qualified legal advice from an expert in the field of personal data protection in particular cases.

IV.
Scope of Application

This Code of Conduct applies to the operators of passenger air transport. They may include individuals and companies, private as well as public sector organizations, non-profit organizations and others. For the purposes of this Code it is not important whether the software used by an airline to facilitate performing a flight for a passenger is administered by the airline itself or is available to it as part of a subcontracted service. However, for the purposes of this Code it is important that the software subcontractor which is defined by the air service provider as a significant contractor is familiarized with this Code or, even better, contractually undertakes to apply it. However, it is worth noting that the European legislation (in the form of either directly applicable Regulations or Directives implemented in national laws) is binding on the providers and that this Code of Conduct must not be inconsistent with such normative legal acts.

V.
Adherence to the Code

The members acceding to this Code share a common objective, namely to facilitate and offer services in the field of civil aviation and the related personal data processing in a transparent and fair manner. The adherence to this Code shall be supervised by the general meeting established by this provision. Each member shall designate one person, either the data controller if appointed or another person appropriate with regard to his or her professional qualities, especially his or her expert knowledge of law and experience in the field of personal data protection. The members shall make sure that the persons designated to participate in the

general meeting in connection with the fulfilment of their tasks are free from any conflict of interest.

This Code is a self-regulatory tool, and the Regulation expects that the adherence to the Code of Conduct will be monitored either by the supervisory authority itself or by a body accredited by the supervisory authority. If this Code is approved by the Office for Personal Data Protection (*Úřad pro ochranu osobních údajů*) or by the Board, the adherence to the Code shall be monitored by a body accredited by the Office for Personal Data Protection and selected by Travel Service, a.s. Until then the monitoring is fully in the hands of the general meeting.

A member of the general meeting may be appointed by any member acceding to the Code for an unlimited time and may also be removed at any time.

The members of the general meeting shall meet once per year in person in the registered office of Travel Service, a.s. where the general meeting is convened by a member of the general meeting designated by Travel Service, a.s., or all members of the general meeting shall discuss the proposed items online once per year. The general meeting shall discuss proposed items, which shall contain, in particular, proposed changes, criticism, interpretation and development of procedures as far as they relate to this Code and to personal data protection. The general meeting shall adopt joint opinions if, based on the discussed agenda, there is a change in the field of personal data processing. The opinions shall be binding on the members acceding to the Code if a joint opinion is adopted by at least 50% of all the members. The convening member must set the date of the meeting or the term for submitting the opinion online, which must not be shorter than 30 days. Introduction of the agenda of the meeting is the first point following the commencement.

VI.

Processing Operations to which This Code Applies

A)

Data controllers collect the following personal data of passengers:

1. name(s) and surname(s),
2. day, month and year of birth,
3. citizenship,
4. number and type of the passport submitted by the passenger,

5. point of entry to the controller's territory,
6. flight number,
7. date and time of departure and arrival,
8. initial boarding point, and
9. total number of passengers travelling on the concerned flight.

A smaller or larger extent of personal data may only be collected by an air carrier if so required from the air carrier by a national legal regulation, or if such collection is lawful according to the personal data protection regulations in the country of the registered office of the air carrier, or if so required from the air carrier by the legislation of the country of departure, flyover or arrival.

These personal data are collected as early as from the moment of booking the flight or, as the case may be, checking-in the passenger.

As part of the preparation of data controllers for the implementation of Directive (EU) 2016/681 of the European Parliament and of the Council on the use of the passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime into national laws, the controllers may collect the following personal data as early as now:

1. PNR record locator
2. Date of reservation/issue of ticket
3. Date(s) of intended travel
4. Name(s)
5. Address and contact information (telephone number, e-mail address)
6. All forms of payment information, including billing address
7. Complete travel itinerary for specific PNR
8. Frequent flyer information
9. Travel agency/travel agent
10. Travel status of passenger, including confirmations, check-in status, no-show or go-show information
11. Split/divided PNR information
12. General remarks (including all available information on unaccompanied minors under 18 years, such as name and gender of the minor, age, language(s) spoken, name and

contact details of guardian on departure and relationship to the minor, name and contact details of guardian on arrival and relationship to the minor, departure and arrival agent)

13. Ticket field information, including ticket number, date of ticket issuance and one-way tickets, automated ticket fare quote fields
14. Seat number or other seat information
15. Code share information
16. All baggage information
17. Number and other names of travellers on the PNR
18. Any advance passenger information (API) data collected (including the type, number, country of issuance and expiry date of any identity document, nationality, family name, given name, gender, date of birth, airline, flight number, departure date, arrival date, departure port, arrival port, departure time and arrival time)
19. All historical changes to the PNR listed in numbers 1 to 18.

These personal data are collected as early as from the moment of booking the flight or, as the case may be, checking-in the passenger.

Controllers may collect personal data related to the health status of a data subject, which are to be collected by the controller under Regulation (EC) No 1107/2006 concerning the rights of disabled persons and persons with reduced mobility when travelling by air. Such personal data, which constitute a special category of personal data, shall be collected by the controller, because they are necessary for the fulfilment of a legal obligation and are subject to derogations from the prohibition for processing referred to in Article 9(2) of GDPR.

Controllers may also collect further personal data related to the health status if this is necessary for proving the compliance with the conditions of carriage (and performance of the contract of carriage) and the obligation to exclude from the carriage such persons, animals and cargo the carriage of which would endanger the aviation safety or the carriage of which would violate the regulations in effect in the state of departure, state of arrival or state of flyover for reasons of substantial public interest, on the basis of Union or Member State law. Such personal data may be data on infarction, stroke, new-born baby, decompression disease, pneumothorax, requirement for a stretcher / travelling with an incubator, necessity to have medical oxygen during the flight, inability to keep a straight posture when sitting, head injury,

fractures (except for non-complicated fractures of upper limbs and fingers of upper limbs), plasters (except for upper limbs and fingers of upper limbs in plaster), severe venous thrombosis, severe mental disease (the passenger must travel with an accompanying person for whom the next seat is secured), or any serious or acute infection disease (including chickenpox), and other personal data on the health status, the processing of which is regarded necessary by the data controller for reasons of substantial public interest, on the basis of Union or Member State law.

B) Having received such information, data controllers shall inform the passengers about:
a) the identity and the contact details of the controller and, where applicable, of the controller's representative
b) the contact details of the data protection officer, where applicable
c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing
d) where the processing is based on point (f) of Article 6(1) of GDPR, the legitimate interests pursued by the controller or by a third party
e) the recipients or categories of recipients of the personal data, if any
f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organization and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1) of GDPR, reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available,
and shall also inform them about:
a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period
b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability
c) where the processing is based on the data subject's consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal
d) the existence of the right to lodge a complaint with a supervisory authority

e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data
f) the existence of automated decision-making, including profiling, and at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subjects.

Where personal data have not been obtained from the data subject, the controller shall also provide the data subject with the information about the category of the concerned personal data and the source from which the personal data originate, and if applicable, whether the data originate from publicly accessible sources.

The information referred to above shall be published by the controllers at least on their websites, so that each data subject has an opportunity to acquaint themselves with them before making a contract or booking a flight.

C) Data minimisation
The personal data referred to in section A) of Article VI) of this Code are minimal, and no further personal data are required for the provision of a transport service. The personal data collected about a passenger on the basis of legal regulations shall be erased by the data controller within 24 hours from the airplane arrival at the final destination, unless the national law sets out a longer storage period for the air carrier.

If the airline needs further personal data for the service provision, it may only require them if the processing is based on a legal ground for the processing that is defined in Article 6 of GDPR. It may also process personal data for a period longer than 24 hours from the airplane arrival at the destination. In order to maintain transparency of processing, each controller may draw up, for the personal data processing based on the legal grounds consisting in the necessity of processing for the purposes of legitimate interests of the controller, a balance test at least to the extent defined in the annex to this Code.

Using its internal organisational and technical measures, the data controller shall ensure that the personal data kept in the data controller’s organisation are only accessible to those

employees who need them for the performance of their work, for a period not longer than needed for the performance of their work.

D) STORAGE LIMITATION/DESTRUCTION

The most fundamental rule to be observed by the air carrier is the destruction of all personal data that are not necessary within 24 hours from the airplane arrival at the final destination, unless a longer period is set out in the national law. The necessity of collecting personal data is due to the compulsory submission of the collected personal data to the competent authority for the purpose of improvement of border control and fighting illegal immigration. After that moment the air carrier may keep those personal data that are processed on lawful grounds for the period transparently set by the carrier itself. A recommended storage period is the general limitation period set out in the laws of the countries of departure, arrival or flyover, or a special limitation period set out for the exercise of rights from the contract of carriage.

E) Transfer of personal data/Transfer of personal data to foreign countries

The air carrier may transfer personal data to

operators of public international airports

handling companies and handling agents

travel offices and travel agencies

national authorities of the countries of arrival, flyover and departure that fulfil the tasks of the state aviation authority

authorities performing public administration in the field of stay of foreigners in the territory of the state of arrival, departure and flyover

other parties participating in the provision of a service consisting in the transport of persons and goods,

but always only if the transfer is necessary for the performance of a contract between the data subject and the controller, or in order to take steps prior to entering into a contract of carriage,

and the air carrier regards an order of a transport service to be a request of the data subject to take such steps.

The air carrier shall make sure that especially where personal data are transferred to third countries there are appropriate safeguards for such transfer as far as possible.

VII.
Procedures to Secure Data Accuracy and Currency

In an internal act, the air carrier shall designate the department which shall secure data accuracy and currency on the basis of a reliably verified input information concerning the accuracy and currency of the data in the carrier's database. One of the input information indicating that data in the carrier's database are inaccurate and out of date may be the exercise of the data subject's right to rectification (Article 16 of GDPR), erasure (Article 17 of GDPR) or restriction of processing (Article 18 of GDPR); after precise evaluation of the conditions of the concerned Articles of the Regulation, the designated department shall secure the data accuracy and currency within 30 days. The department shall always create an internal record thereof.

VIII.
Procedures to Secure Lawfulness of Processing

Each personal data processing must be stated in the records of processing activities, the minimal scope of which is described in an annex to this Code, and such records shall be kept by the department designated in the internal act. If complying with the processing rules under the provisions of Article 6 of GDPR, the air carrier will be sure of the lawfulness of such processing.

A new record of processing activities shall always be created by the air carrier when:

a) the controller plans to begin to collect new personal data that have not been collected before
b) the controller begins to process personal data in a different manner
c) the controller plans to begin to process any of the collected personal data for a purpose other than for which it has originally been collected.

In an event referred to in subparagraph b) of Article VIII, the controller shall carry out a proportionality test, while taking into account, in particular, whether the processing for a different purpose is compatible with the original purposes. The controller shall create a record thereof.

Afterwards, the controller shall update the information obligations towards the data subjects or inform the data subjects of the new purpose of processing.

IX.
Procedures to Secure Consent of the Data Subject

As far as possible, the controllers shall consider the lawfulness of processing based on the data subject's consent as a marginally used legal ground and shall always try to process only such personal data that are necessary for the performance of activities in the field of air transport, either for the performance of a contract to which the data subject is a party, for the fulfilment of a legal obligation, or for the protection of vital interests of the data subject, or for the fulfilment of a task carried out in public interest, or where such processing is necessary for the purposes of legitimate interests pursued by the concerned controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

If the processing is based on consent, the controller must be able to prove that the data subject has given consent to the personal data processing. This may be proven by the controller through "logging-in" or by means of a signature attached to the written declaration of the data subject's consent to the personal data processing. The consent must be distinguishable from other matters, must be in an intelligible and accessible form, using clear and plain language, and must be free, and the text of the consent must inform the data subject whether the performance of the contract is conditional on such consent. The controller shall make sure that the data subject who has given consent receives information about:

a) the identity and contact details of the controller and, where applicable, of the controller's representative

b) the contact details of the data protection officer, where applicable

c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing

d) where the processing is based on point (f) of Article 6(1) of GDPR, the legitimate interests pursued by the controller or by a third party

e) the recipients or categories of recipients of the personal data, if any

f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organization and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1) of GDPR, reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available,

and shall also inform them about:

a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period

b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability

c) where the processing is based on the data subject's consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal

d) the right to lodge a complaint with a supervisory authority

e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data

f) the existence of automated decision-making, including profiling, and at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subjects.

X.

Procedures to Secure Awareness of Data Subjects and Public

The controller shall take appropriate measures to provide the data subject, in a concise, transparent, intelligible and easily accessible form, using clear and plain language, with any information referred to in Articles 13 and 14 of GDPR (see paragraph B) of Article VI of the Code) and information about the data subject's rights to access to personal data, to rectification, to erasure, to restriction of processing, to object to processing and the data subject's right not to be subject to a decision based solely on automated processing, including

profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. If the data subject exercises his or her right to the rectification or erasure or restriction of processing concerning his or her personal data, the controller shall communicate this fact to each recipient, unless this proves impossible or involves disproportionate effort.

The controller must publish the information required by the Regulation on its website and other places where appropriate.

The controller shall communicate personal data breaches to the supervisory authority, except for a situation where the breach is unlikely to result in a risk to the rights and freedoms of natural persons, within 72 hours after having become aware of it.

The controller shall communicate a personal data breach to the data subject if such breach is likely to result in a risk to the rights and freedoms of natural persons. The controller shall draw up a catalogue of risks and a catalogue of personal data breaches, which shall serve as a guideline for the notification obligation set out by the Regulation and this Code.

XI.
Procedures to Secure and Exercise Data Subjects' Rights

XI.A) Right to access to personal data

The data subject has the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and to the information referred to in an annex to this Code. The controller shall make the personal data available to the data subject either in the form defined in the annex or in another similar manner within 30 days from the date of receipt of the request. A precondition for granting access to the personal data is a sufficient identification of the person requesting the access. The controller shall designate the particular persons or department to safeguard the exercise of the data subject's right.

XI.B) Right to rectification

The data subject has the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. The controller shall communicate the rectification to the data subject within 30 days from the day of receipt of the request, but shall rectify the data without undue delay. A precondition for the rectification of the personal data is a sufficient identification of the person requesting the rectification. The

controller shall designate the particular persons or department to safeguard the exercise of the data subject's right.

XI.C) Right to erasure ("right to be forgotten")

The data subject has the right to obtain from the controller the erasure of personal data concerning him or her. In such case the controller shall assess whether:

- the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed
- the data subject has withdrawn consent to the processing of personal data and there is no other legal ground for the processing
- the data subject has objected to the processing and there are no overriding legitimate grounds for the processing (note: if the data subject objects to the personal data processing for direct marketing purposes, no serious legitimate grounds can be inferred)
- the personal data have not been unlawfully processed
- the personal data have to be erased for compliance with a legal obligation set out in Union or Member State law to which the controller is subject
- the personal data have been collected in relation to the offer of information society services to a child of an age set out by the national legislation for personal data protection at the controller,

and shall either comply or not comply with the request to exercise the right to erasure. In any case, however, the controller shall inform the data subject about the result of safeguarding his or her right within 30 days. A precondition for the erasure of the personal data is a sufficient identification of the person requesting the erasure. The controller shall designate the particular persons or department to safeguard the exercise of the data subject's right.

The right to erasure may not be exercised if the processing is necessary:

a) for exercising the right of freedom of expression and information;
b) for compliance with a legal obligation
c) for reasons of public interest in the area of public health
d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes
e) for the establishment, exercise or defence of legal claims.

XI.D) Right to restriction of personal data processing

Restriction of processing means mere storage of the personal data in a manner not allowing further processing. Exceptionally, such restricted personal data may be processed for the purpose of establishment, exercise or defence of legal claims, for the protection of another person's rights or for reasons of important public interest. They may also be processed with the data subject's consent.

The data subject may contest accuracy of personal data or object to the processing of personal data, and in order to verify the accuracy or to verify any overriding interests of the controller or the data subject, the controller shall restrict their processing for a period not exceeding 30 days from the receipt of the request exercising the right. The same procedure shall be taken by the controller if the personal data processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their processing, or the data subject requires such data for the establishment, exercise or defence of legal claims.
The data subject shall be informed by the controller about the restriction of processing and about lifting the restriction of processing.

A precondition for the restriction of personal data processing is a sufficient identification of the person requesting the restriction of processing. The controller shall designate the particular persons or department to safeguard the exercise of the data subject's right.

Common point for XI.B); C); D) – If possible, the controller shall communicate to all the recipients to whom the personal data of a data subject were disclosed that the data subject's request to exercise his or her rights referred to in these Articles of the Code has been complied with.

XI.E) Right to data portability

At a passenger's request, the air carrier shall provide the passenger with all the personal data concerning him or her, which he or she has provided to the controller, in a commonly used and machine-readable format directly to the passenger or to another data controller where technically feasible, if the processing is carried out by automated means and, at the same time, is based on the data subject's consent or is necessary for the performance of a contract to

which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract.

XI.F) Right to object to personal data processing

If the air carrier processes personal data for direct marketing purposes, the passenger or another person may object to the processing of personal data concerning him or her, and the air carrier shall accept the objection without further consideration and shall no longer process the personal data for direct marketing purposes.

The passenger also has the right to object to personal data processing if the air carrier declares that it processes personal data on the basis of its legitimate interest or that the processing is necessary for the performance of tasks carried out for reasons of public interest or if the passenger believes that this should be declared by the carrier in that way. The air carrier has to assess whether its interests (or public interests) override the interests or fundamental rights and freedoms of passengers, and if the passenger's rights are overriding, the air carrier has to accept the objection.

XI.G) Right not to be subject to a decision based solely on automated processing

Each air carrier shall assess the necessity to introduce automated individual decision-making, including profiling, into its processes and shall always, if possible, prefer an individual approach to the entire process of personal data processing. If the air carrier decides solely by automated means, including profiling, it shall make sure to provide transparent information to data subjects and respect the right of a data subject not to be subject to such processing and decision-making.

XI.H) Right to lodge a complaint with the Office for Personal Data Protection (*Úřad pro ochranu osobních údajů*) and the right to a judicial remedy against the controller or processor.

Each air carrier shall inform its passengers, without any exception whatsoever, about the possibility of lodging a complaint with supervisory authorities or the possibility of exercising their rights to a judicial remedy before a court.

XII.

Procedures to Safeguard the Security of Personal Data

With regard to the main purpose of this Code, which is to clarify the context of personal data processing for the passengers, this article describes the basic structure of safeguarding the security of personal data, which consists of:

- the security assessment
- a set of technical and organisational measures (e.g. control of physical access, control of logic access, safeguarding the readability of personal data for authorised persons (including encryption), logging and monitoring, use of identification and authentication, use of passwords, security of the communication environment, safeguarding the functionality, backing-up, archiving, operation continuity / restoration after emergency, destruction of data and data carriers, personnel measures, etc.),
- the method and periodicity of the verification of efficiency of implemented technical and organisational measures,
- security safeguarding documentation (e.g. security policy, risk analysis and personal data protection impact assessment, documentation of technical and organisational measures, documentation of the product development, and the inventory of hardware, software, services, data and media, etc.).

XIII.

Procedures in the Personal Data Processing by a Controller or Processor Established outside the EU, if taking place

This Code is only intended for controllers established in the EU. If personal data are going to be processed by a processor outside the EU, the controller shall assess whether the processing is possible based on the points ranked in descending order of priority, and if the controller does not find a match in any case, it shall declare such processing impossible and shall not process personal data through the selected processor. Such assessment shall always be carried out by the controller before commencement of the intended processing.

XIII.1) Transfers on the basis of an adequacy decision

The air carrier shall find out whether there is an adequacy decision of the Commission (EU) in which the Commission stated that the country of the personal data recipient ensures an adequate level of personal data protection. If there is such a decision, the air carrier considers the transfer to be secure. If there is no such decision, the air carrier shall find out whether transfers are taking place subject to appropriate safeguards.

XIII.2) Transfers subject to appropriate safeguards

As appropriate safeguards, the air carrier shall accept, without further consideration, the codes of conduct or the binding corporate rules approved by the supervisory authority or the certificates of personal data protection if such documents refer to the mechanism of transfer and if their wording has been approved by the authority. Until the documents referred to in the preceding sentence have been approved, the air carrier shall ensure using standard "export" clauses of personal data protection, namely under the Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council.

XIII.3) Derogations for specific situations

In the absence of an adequacy decision or appropriate safeguards, transfers may only take place on one of the following conditions:

a) the passenger has consented to the transfer, after having been informed of the possible risks of such transfers for him or her due to the absence of an adequacy decision and appropriate safeguards;
b) the transfer is necessary for the performance of the contract of carriage made between the passenger and the air carrier or for the implementation of measures at the data subject's request prior to making the contract of carriage (where the flight booking itself is already deemed to be such a request) or for the performance of the contract of carriage which was made in the interest of the passenger;
c) the transfer is necessary for important reasons of public interest;

d) the transfer is necessary to protect the vital interests of the passenger, where the passenger is physically or legally incapable of giving consent;
e) the transfer is necessary for the establishment, exercise or defence of legal claims;
f) the transfer is made from a public register established under Union law and intended to provide information to the public.

XIII.4 Single transfer in absence of decision, appropriate safeguard and applicable derogation

Where there is no adequacy decision by the Commission or appropriate safeguards and where none of the derogations for specific situations is applicable, the controller may transfer personal data if:

a) the transfer is not repetitive
b) the transfer concerns only a limited number of data subjects
c) the transfer is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests of the passenger
d) the controller has assessed all the circumstances surrounding the data transfer and provided all conceivable suitable safeguards for the transfer
e) the controller has provided the passenger and the supervisory authority with information about such single transfer and all related information.

XIV.
Procedures for Monitoring the Code of Conduct at the Controller or Processor

This Code of Conduct may be monitored by:

a) a representative of Travel Service, a.s. until the Code of Conduct has been approved by the supervisory authority; such monitoring is not monitoring of an approved code of conduct under Article 41 of GDPR, in particular due to the absence of approval of the Code and the absence of independence
b) the supervisory authority after the moment of the Code approval by the supervisory authority
c) a body accredited by the supervisory authority after the moment of the Code approval by the supervisory authority.

XV.

Model Clause Containing the Entity's Obligation to Adhere to the Code and to Secure the Monitoring of the Code, and where Applicable, to Pursue Further Cooperation with the Accredited Body

The contracting party hereby undertakes to comply with the Code of Conduct approved under Article 40 of GDPR. Until the Code of Conduct referred to in the preceding sentence is approved by the Authority, the contracting party shall adhere to the Code of Conduct published on the website https://www.travelservice.aero/o-spolecnosti/ochrana-osobnich-udaju/.

ANNEXES

MODEL – RECORDS OF PROCESSING ACTIVITIES

(including a catalogue of personal data and general risk assessment)

MODEL – CATALOGUE OF RISKS

MODEL – Balance test for the assessment of a legitimate interest

MODEL – Giving the data subject access to personal data

MODEL – Notification obligation regarding rectification or erasure of personal data or restriction of processing

MODEL – Identification of a data breach and assessment of incident risks

MODEL – Report of notification of a personal data breach to the supervisory authority

MODEL – Personal data protection impact assessment

ANNEX – RECORDS OF PROCESSING ACTIVITIES

Identification and contact details (*point (a) of Article 30(1) of GDPR*)	***Company / name and surname***	***ID***	***Permanent residence / registered office***	***E-mail***	***Telephone***
Controller					
Controller's representative					

Data subject	**Purposes of processing (*point (b) of Article 30(1) of GDPR*) Purpose limitation (*point (b) of Article 5(1) of GDPR*)**	**Lawfulness of processing (point (a) of Article 5(1) of GDPR)** (legal grounds - e.g. consent, legitimate interest, legal obligation (specify), etc.)	**Categories of data subjects (*point (c) of Article 30(1) of GDPR*)**	**Categories of personal data (point (c) of Article 30(1) of GDPR)**	**Contents of the data set**

Source of personal data	**Time limit for erasure of personal data (point (f) of Article 30(1) of GDPR) Storage limitation (point (e) of Article 5(1) of GDPR)**	**Categories of recipients (point (d) of Article 30(1) of GDPR)**	**Transfer of personal data to a third country or international organisation (point (e) of Article 30(1) of GDPR)**

Description of technical and organisational measures (point (g) of Article 30(1) of GDPR) Integrity and confidentiality (point (f) of Article 5(1) of GDPR) (e.g. under Article 32(1) of GDPR: pseudonymisation, encryption, availability, confidentiality, integrity and resilience of the system, restored availability, regular testing, assessment and evaluation)	**Data minimisation (point (c) of Article 5(1) of GDPR)**	**Accuracy (point (d) of Article 5(1) of GDPR)**	**Risk evaluation (higher than level 1)**

ANNEX – MODEL – CATALOGUE OF RISKS

Group		Subgroup		Risk evaluation
A	Human factor risks	A-1	Theft of property including a personal data carrier caused by an employee	
		A-2	Misuse of information and personal data	
		A-3	Lack of knowledge and training of employees	
		A-4	Non-compliance with the employee Code of Conduct	
		A-5	Carelessness	
		A-6	Addiction to habit-forming substances	
B	Property security risks	B-1	Security guarding of the building	
		B-2	Theft or loss of mobile devices	
		B-3	Security of passwords	
		B-4	Security of archives	
C	Operational risks	C-1	Non-observance of approved procedures	
		C-2	Inaccuracy of work procedures	
		C-3	Inadequacy of remedial measures	
		C-4	Performance of incompatible procedures/processes	
		C-5	Complicacy of operations	
		C-6	Complicacy of standards and rules	
		C-7	Absence of control	
D	Organisational risks	D-1	Internal and external reporting	
		D-2	Circulation of documents, recording, destruction	
		D-3	Risk of leak of personal data during transfers of persona data of various departments	
		D-4	Risk of leak of personal data during transfers to third parties	
		D-5	Risk of leak of personal data during receipt from third parties	
		D-6	Security of provided personal data at third parties	
E	Legal risks	E-1	Contractual clauses – clauses of confidentiality and protection of personal data	
		E-2	Non-observance of binding regulations	
		E-3	Absence of processing contracts	
		E-4	Personal data protection with respect to the laws of the relevant destinations	
F	Information and technological risks	F-1	Access rights	
		F-2	Integrity of systems and applications	
		F-3	Interconnection of systems	
		F-4	Physical security of data and their protection	
		F-5	Accessibility of information systems	
		F-6	Security of information systems	
		F-7	Administration of network applications	
		F-8	Security of systems and applications	
		F-9	Security of servers and storage of information	

ANNEX – MODEL – Balance test for the assessment of a legitimate interest

Name: **(***e.g. Keeping the general personal data of passengers of regular carriage – names, surnames, dates of birth for a period exceeding 24 hours***).**

I. Identification of a legitimate interest

a. What is the purpose of processing?

b. For how long will the data be processed?

c. Is the processing necessary for the achievement of certain objectives of the controller or a third party?

d. Are these data provided to a third party?

II. Necessity test

a. Why is the processing important for the controller?

b. Is it necessary to process the data to the concerned extent?

c. Why is the processing important for other recipients of the data, if any?

d. Are there any alternative ways to reach the objective without using these data?

III. Balance test

a. Can it be generally expected that such data processing will be carried out?

b. Is the data processing associated with an added value to a service used by the subject?

c. Is it likely that the data processing will have a negative impact on the subject's rights?

d. Is it likely that the data processing will cause unjustified detriment to the subject?

IV. Conclusion

ANNEX – MODEL – **Giving the data subject access to personal data**

This document is drawn up in accordance with Article 15 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Name and contact details of the data subject:

(Data subject)
(Contact details if available)

Name and contact details of DPO/other contact point for the provision of information:

(DPO/gestor/authorised person where DPO is designated)

We confirm that we process the following personal data of yours:

(List of the personal data being processed under Article 15(1))

We are providing you with the following additional information:
a) the purposes of the personal data processing:
b) the categories of the personal data concerned:
c) the categories of recipients to whom the personal data have been disclosed:
f) the source of the personal data is:
d) you have the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing
e) you have the right to lodge a complaint with a supervisory authority, which is the Office for Personal Data Protection (*Úřad pro ochranu osobních údajů*)
g) existence/absence of automated processing of the personal data
h) the personal data have/have not been transferred to third countries

Attachment:
Copy of the personal data being processed:

Place:……. Date: …….

CARRIER'S NAME

ANNEX – MODEL – **Notification obligation regarding rectification or erasure of personal data or restriction of processing**

This communication was sent to you in accordance with Article 19 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Name and contact details of the data subject:

(Data subject)
(Contact details if available)

Name and contact details of DPO/other contact point for the provision of information:

(DPO/gestor/authorised person where DPO is designated)

Reason for the communication:

(The reason for which the rectification/erasure/restriction of processing of the personal data took place)

List of the personal data which are the subject of the communication:

(A list of the personal data that were rectified or erased or that are subject to restriction of processing)

Place:……. Date: …….

ANNEX – MODEL – **Identification of a data breach and assessment of incident risks**

Identification and assessment of incidents are carried out under Article 32 “Security of processing” and Article 35 “Data protection impact assessment” of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Name and contact details of the controller:

(Organisation/person)
(Registered office/contact details)

Name and contact details of DPO/other contact point for the provision of information:

(DPO/gestor/authorised person)

Procedure to be taken in the event of identification of a data breach and the assessment incident risks

1. Description of the incident:

(Detailed description of the event involving the loss/theft/misuse/consultation of personal data by an unauthorised person. Description and categories of stolen/lost personal data. Description of effects of the breach associated with the loss/theft/misuse/consultation of personal data by an unauthorised person)

2. Description of risks associated with the loss of personal data of the data subject:

(Detailed description of the risks that may be faced by the data subject due to the loss/theft of the personal data as described in point 1.)

3. Description of remedial measures taken for the protection of the data subject:

(Detailed description of the remedial measures, their implementation and impact, based on the descriptions in points 1 and 2)

Notification/communication of the incident:

a) Are the risks still relevant even after the remedial measures have been taken?

- **Yes** – The incident has to be notified to the supervisory authority. The data subject shall be notified of the incident only in the event of a high risk to his or her rights and freedoms. To notify the incident, it is possible to use the document "Notification of a personal data breach to the supervisory authority", or this document may be used with a change of the addressee for the communication to the data subject.
- **No** – The incident does not have to be notified. (It is necessary to give relevant reasons why the incident was not notified – see point 3).

Place:…….

Date: …….

……
(Signature of the controller)

……
Signature of the data protection officer/authorised person

ANNEX – MODEL – **Report of notification of a personal data breach to the supervisory authority**

This report is drawn up on the basis of Articles 33 and 34 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Name and contact details of the controller:

(Organisation/person)
(Registered office/contact details)

Name and contact details of DPO/other contact point for the provision of information:

(DPO/gestor/authorised person)

Description of the personal data breach:

1. Nature of the personal data breach:

2. Categories and approximate number of the data subjects concerned (where it is possible to state them):

3. Categories and approximate number of the personal data records concerned (where it is possible to state them):

Description of likely consequences and description of measures taken or proposed to be taken:

Likely consequences of the personal data breach:

Measures taken and proposed to be taken to address the personal data breach:

Place:…….

Date: …….

……

(Signature)

ANNEX – MODEL – **Personal data protection impact assessment**

This document is drawn up in accordance with Article 35 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Name and contact details of the controller:

(Organisation/person)
(Registered office/contact details)

Name and contact details of DPO/other contact point for the provision of information:

(DPO/gestor/authorised person where DPO is designated)

Advice from the data protection officer:

(Advice from DPO)
(The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment)

Impact assessment:

1. Description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interests pursued by the controller:

It is possible to quote the information stated in the catalogue of personal data (see annex No. 1 to the Code)

2. Assessment of the necessity and proportionality of the processing operations in relation to the purposes:

It is possible to quote the information stated in the catalogue of personal data (see annex No. 1 to the Code)

3. Assessment of the risks to the rights and freedoms of data subjects:

It is possible to quote the information stated in the catalogue of risks (see annex No. 2 to the Code)

4. Measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned:

It is possible to quote the information stated in the catalogue of risks (see annex No. 2 to the Code)

View of the data subjects or their representatives:

(Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations)

Place:……. Date: …….

……

(Signature)