Text consolidated by Valsts valodas centrs (State Language Centre) with amending laws of:

10 May 2018 [shall come into force from 25 May 2018];

24 October 2019 [shall come into force from 20 November 2019];

20 January 2022 [shall come into force from 17 February 2022].

If a whole or part of a section has been amended, the date of the amending law appears in square brackets at the end of the section. If a whole section, paragraph or clause has been deleted, the date of the deletion appears in square brackets beside the deleted section, paragraph or clause.

The *Saeima*1 has adopted and

the President has proclaimed the following law:

**Aircraft Passenger Data Processing Law**

**Chapter I**

**General Provisions**

**Section 1. Terms Used in this Law**

(1) The following terms are used in this Law:

1) **intra-EU flight**– an international flight the origin or stop-over of which is in another Member State within the meaning of Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (hereinafter – the Member State) but the stop-over or destination of which is planned in the territory of Latvia or the origin or stop-over of which is in the territory of Latvia but the stop-over or destination of which is in another Member State;

2) **extra-EU flight**– an international flight the origin or stop-over of which is in a country that is not a Member State (hereinafter – the third country) but the stop-over or destination of which is planned in the territory of Latvia, or the origin or stop-over of which is in the territory of Latvia but the stop-over or destination of which is in a third country;

3) **air carrier**– a person with a valid operating licence or an equivalent document permitting it to carry out commercial flight of passengers by air;

4) **passenger**– any person, excluding members of the aircrew, carried or to be carried in an aircraft with the consent of the air carrier, which is manifested by that person’s registration in the passengers list;

5) **passenger data**– information which is processed by air carriers’ reservation systems, departure control systems (systems which are used to check passengers onto flights), or equivalent systems to ensure the processing and control of flight reservations booked by a person or on his or her behalf;

6) **Passenger information unit**– a structural unit of the State Security Service assigned for the processing of passenger data.

(2) Within the meaning of this Law, the term “serious crimes” shall mean the criminal offences referred to in Annex to this Law for the committing of which deprivation of liberty or a security measure related to the deprivation of liberty is applied and the maximum duration of which is at least three years in accordance with the laws and regulations of a Member State.

[*10 May 2018; 24 October 2019*]

**Section 2. Purpose of the Law**

The purpose of the Law is to ensure the processing of passenger data which is necessary to perform analysis for the prevention and detection of crimes related to terrorism and serious crimes, and also for the prevention of threats to national security.

[*10 May 2018*]

**Section 3. Manager and Keeper of the Register and Tasks of the Register**

(1) Aircraft passenger data register (hereinafter – the Register) is a State information system the manager and keeper of which is the State Security Service. The Information Centre of the Ministry of the Interior shall ensure the functionality of the technical resources of the Register.

(2) The Register shall provide institutions with an opportunity to receive the passenger data included therein which are necessary for the prevention and detection of crimes related to terrorism and serious crimes, for the prevention of threats to national security, and also for minimising the spread of such infectious disease endangering public health and to be registered for which an epidemiological investigation should be performed.

[*10 May 2018; 24 October 2019; 20 January 2022*]

**Chapter II**

**Information to be Included in the Register, Procedure for the Inclusion Thereof and its Storage**

**Section 4. Information to be Included in the Register**

The following information shall be included in the Register:

1) passenger name record locator;

2) date of reservation and issue of ticket;

3) date of the intended travel;

4) given name, surname of a passenger;

5) address and contact information of the passenger (telephone number, e-mail address);

6) payment information and also billing address;

7) information regarding the route of a specific flight;

8) type, number and owner of the loyalty card;

9) travel agency and travel agent;

10) status of the passenger during the travel, including, the check-in status, information on the no-show or go-show;

11) information on split/divided reservations;

12) general remarks which do not contain special categories of personal data (for example, a note that the child travels unaccompanied, the language in which he or she speaks, name and contact details of guardian on departure and relationship thereof to the minor, name and contact details of guardian on arrival and relationship thereof to the minor, departure and arrival agent);

13) ticket number, date of ticket issuance and one-way tickets, automated ticket fare quote fields;

14) seat number;

15) code share information;

16) information on the checked baggage of the passenger which is available in the departure control system – number of units and weight, identification number, code of the baggage carriers, baggage status (for example, checked in, delivered, stolen, damaged, confiscated), place of baggage delivery;

17) number, names and surnames of passengers of other aircrafts of the same passenger name record locator;

18) all data of the advance passenger information (type, number, country of issuance, and expiry date of the travel document of a passenger, citizenship, given name, surname, sex, date of birth, air carrier, flight number, time of departure and arrival, airport of departure and arrival, date of departure and arrival, the border crossing point of entry into the territory of the State through which the passenger will enter the Republic of Latvia, the number of other aircraft passengers);

19) [10 May 2018];

20) all historical changes to the data laid down in this Section.

[*10 May 2018*]

**Section 5. Obligation of Air Carriers to Transfer Passenger Data for the Automated Inclusion Thereof in the Register**

(1) In relation to an extra-EU flight or an intra-EU flight an air carrier has an obligation to transfer the passenger data referred to in Section 4 of this Law to the extent that the air carrier processes them in the context of its commercial operations in order to provide air transport services for the automated inclusion (hereinafter – the inclusion) thereof in the Register not sooner than 48 hours and not later than 24 hours before the scheduled time for flight departure and immediately after the flight closure, when the boarding and alighting of passengers are no longer possible.

(2) [24 October 2019]

(3) If changes are made to the passenger data which have been transferred for the inclusion in the Register in accordance with Paragraph one of this Section, the air carrier shall transfer the relevant data after the flight closure, when the boarding and alighting of passengers are no longer possible.

(4) In case where immediate action is required to prevent a terrorist attack or a real threat to the life or health of a person and a request of the Passenger information unit has been received to provide passenger data, an air carrier shall send the required passenger data for the inclusion thereof in the Register within the time period specified in the request which is not shorter than four hours.

(5) Where the flight is code-shared between one or more air carriers, the obligation to transfer the data of all passengers on the flight for the inclusion thereof in the Register shall be on the air carrier that operates the flight.

(6) The Cabinet shall lay down requirements regarding the transferring of passenger data and inclusion thereof in the Register.

[*24 October 2019* / *See Paragraph 3 of Transitional Provisions*]

**Section 6. Right of the Passenger Information Unit to Request the Transferring of Passenger Data for the Inclusion Thereof in the Register**

[24 October 2019]

**Section 7. Depersonalisation of Passenger Data**

(1) The passenger data which have been retained in the Register for six months after their inclusion therein shall be depersonalised by masking out (by making them invisible rather than deleting) the following personal identification information:

1) given name, surname;

2) address and contact information;

3) payment information and billing address, if such information can be used to identify the person;

4) type, number and owner of the loyalty card;

5) general remarks specified in Section 4, Clause 12 of this Law, insofar as they can be used to identify the person;

6) all data of the advance passenger information, except for the following data:

a) the border crossing point of entry into the territory of the State through which the passenger will enter the Republic of Latvia;

b) flight number;

c) time of departure and arrival of the aircraft;

d) total number of passengers on the aircraft;

e) country of issuance and expiry date of the travel document;

f) sex of the passenger;

g) air carrier.

(2) If it is necessary to obtain passenger data included in the Register for the prevention and detection of crimes related to terrorism, serious crimes, or for the prevention of threats to national security, the Passenger information unit has, after receipt of the consent of a judge to issue passenger data upon request of an institution, the right to personalise the depersonalised passenger data and issue them in the requested amount to the relevant institution.

[*10 May 2018*]

**Section 8. Passenger Data Retention Period**

The passenger data shall be retained in the Register for five years from the day of inclusion thereof, but after the abovementioned period they shall be automatically and permanently deleted.

[*24 October 2019*]

**Chapter III**

**Issuance of Passenger Data**

**Section 9. Automated Processing of Passenger Data in the Register**

(1) The data included in the Register on a person (name, surname, sex, date of birth, citizenship), travel document (type, number, country of issuance and expiry date of the document) and means of payment (type of the means of payment, number and expiry date of the payment card) are examined automatically by comparing them against the relevant data on persons, travel documents and means of payment included in the following information systems:

1) Register of Ascertaining the Location of a Person, Property or Document of the Integrated Interior Information System;

2) the sub-system “Invalid Document Register” of the Integrated Information System of the Interior;

3) Schengen Information System;

4) International Criminal Police Organisation (Interpol) database of Stolen and Lost Travel Documents (SLTD);

5) databases of the International Criminal Police Organisation (Interpol) in relation to wanted persons.

(2) The Register shall transfer to the Passenger information unit an automatic notification of a match established in an automated data processing by indicating the passenger data that are included in the Register in relation to the relevant entry.

(3) In the processing of data included in the automatic notification of the Register the Passenger information unit shall ascertain the accuracy of the automated processing in the relevant information system. When the Passenger information unit has ascertained the conformity of data, it shall act by complying with the laws and regulations governing the operation of information systems referred to in Paragraph one of this Section.

(4) An automated processing result not approved in the individual processing may be retained until the underlying passenger data are deleted.

[*10 May 2018*]

**Section 10. Right to Request Passenger Data**

If there are grounds to believe that the passenger data may help to prevent or detect crimes related to terrorism or serious crimes, or to prevent threats to national security, the following institutions have, according to their competence, the right to request to issue passenger data included in the Register after receipt of the consent of a judge:

1) the State Security Service;

2) the State Police;

3) the State Border Guard;

4) the Internal Security Office;

5) the Corruption Prevention and Combating Bureau;

6) the Military Police;

7) the Military Intelligence and Security Service;

8) the Constitution Protection Bureau;

9) the Tax and Customs Police, the Internal Security Office of the State Revenue Service;

10) the Office of the Prosecutor.

[*10 May 2018; 24 October 2019*]

**Section 11. Request of an Institution to Issue the Passenger Data**

To receive the passenger data from the Register the institutions referred to in Section 10 of this Law shall turn to a district (city) court based on the location of the institution with a written request. The following shall be indicated in the request:

1) the name, surname and position of the official making the request. State intelligence and security services for which indication of the information referred to in this Clause would constitute a disclosure of an official secret shall indicate their name in the request;

2) the time period (not longer than six months) for which the passenger data that will be included in the Register must be received, starting from the following day after the consent of a judge;

21) the time period for which the respective data are required if it is necessary to receive the data already included in the Register;

3) justification of the need for passenger data;

4) the objective to be achieved;

5) the reason which prevents the achievement of the objective or significantly hinders it, if the passenger data will not be issued;

6) selection criteria for the acquisition of the required information referred to in Section 4 of this Law.

[*20 January 2022*]

**Section 12. Consent of a Judge to the Issuance of Passenger Data**

(1) In order to give the consent to the issuance of passenger data from the Register a judge shall become acquainted with the request referred to in Section 11 of this Law and, if necessary, other materials on the basis of which the request is justified.

(2) A judge shall draw up the consent to the issuance of passenger data and also the refusal as a separate document or resolution. The decision of a judge may not be appealed.

(3) A judge may extend the given consent for six months if the grounds indicated for the receipt of passenger data from the Register have not ceased to exist. A judge has the right to extend the time period for the receipt of passenger data unlimited times.

**Section 13. Execution of a Request for the Issuance of Passenger Data**

(1) The institution referred to in Section 10 of this law shall, within 10 working days after the day when the consent of a judge has been received, submit to the Passenger information unit a request to issue passenger data. If the institution has not complied with the laid down time period, the Passenger information unit shall refuse to issue the requested passenger data.

(2) The passenger information unit shall, within 30 days after the day of the receipt of the request submitted in the time period which is laid down in Paragraph one of this Section, issue the requested passenger data to the institution or include in the Register the information selection criteria indicated in the request, if passenger data which are not yet included in the Register are requested.

(3) If the grounds to request and receive passenger data have ceased to exist, the institution which requested them shall immediately inform the Passenger information unit.

(4) If the grounds to request and receive passenger data have ceased to exist, the Passenger information unit shall immediately terminate issuance thereof to the relevant institution.

**Section 14. Issuance of Passenger Data in Urgent Cases**

(1) In cases where immediate action is required to prevent terrorist attacks or a real threat to the life or health of a person the Passenger information unit has the right to issue passenger data from the Register without the consent of a judge.

(2) To receive passenger data from the Register in accordance with Paragraph one of this Section the institutions referred to in Paragraph 10 of this Law shall turn to the Passenger information unit with a request. The following shall be indicated in the request:

1) the name, surname and position of the official making the request. State intelligence and security services for which indication of the information referred to in this Clause would constitute a disclosure of an official secret shall indicate their name in the request;

2) the justification of the urgency for the receipt of the requested passenger data and time period for which the requested passenger data is to be received;

3) selection criteria for the acquisition of the required information referred to in Section 4 of this Law.

(3) The Passenger information unit shall refuse to issue the requested passenger data, if the information referred to in Paragraph two of this Section has not been included in the request.

(4) The institution which submitted the request shall inform a district (city) court based on the location of the institution regarding the issue of passenger data from the Register not later than within 72 hours, by indicating the justification of the urgency for the receipt of passenger data and also the information referred to in Section 11 of this Law.

(5) A judge shall evaluate the justification of a request of an institution and data issuance and draw up the decision as a separate document or resolution. The decision of a judge may not be appealed.

(6) If the judge has determined that a request of an institution and issuance of passenger data is unjustified, the relevant institution shall inform the Passenger information unit thereof and immediately delete the received passenger data.

(7) The Passenger information unit shall terminate the issuance of passenger data from the Register if the consent of a judge has not been received within 72 hours.

**Section 14.1 Issuance of Passenger Data without the Consent of a Judge**

(1) If the connection of a particular person to a crime related to terrorism or to the committing, preparation, or attempt to commit a serious crime or threats to national security has been previously identified and substantiated, the institutions referred to in Section 10 of this Law have the right, not more than once every six months, with the consent of the head of the respective institution or an official authorised by him or her (without the consent of a judge), to submit a written request to the Passenger information unit to issue only the following information referred to in Section 4 of this Law, included or to be included in the Register, on a particular and previously identified journey (flight or split/divided reservations) of the respective person insofar there are reasonable grounds for considering that obtaining of the requested amount of information may help to prevent or detect the abovementioned crime or to prevent threats to national security:

1) passenger name record locator;

2) date of reservation and issue of ticket;

3) date of the intended travel;

4) given name, surname of a passenger;

5) address and contact information of the passenger (telephone number, e-mail address);

6) information regarding the route of a specific flight;

7) travel agency and travel agent;

8) status of the passenger during the travel, including, the check-in status, information on the no-show or go-show;

9) information on split/divided reservations;

10) general remarks which do not contain personal data of special categories regarding the language in which the passenger speaks;

11) ticket number, date of ticket issuance and one-way tickets, automated ticket fare quote fields;

12) code share information;

13) data of the advance passenger information (type, number, country of issuance, and expiry date of the travel document of a passenger, citizenship, sex, date of birth, air carrier, flight number, time of departure and arrival, airport of departure and arrival, date of departure and arrival, border crossing point of entry into the territory of the State through which the passenger will enter the Republic of Latvia, the number of other aircraft passengers).

(2) If the likelihood of a particular person getting infected with an infectious disease to be registered for which an epidemiological investigation should be performed or the likelihood of the person having been in contact with such infected person has been previously identified and substantiated, the Centre for Disease Prevention and Control has the right, with the consent of the head of the institution or an official authorised by him or her (without the consent of a judge), to submit a written request to the Passenger information unit to issue only the following information referred to in Section 4 of this Law on a particular and previously identified journey (flight or split/divided reservations) of the respective person which has been included in the Register not earlier than within the last three months from the date of submitting the request insofar as there are reasonable grounds to consider that obtaining of the requested amount of information may help to prevent threats to public health:

1) date of the intended travel;

2) given name, surname of a passenger;

3) address and contact information of the passenger (telephone number, e-mail address);

4) information regarding the route of a specific flight;

5) data of the advance passenger information ( date of birth of the passenger, air carrier, flight number, time of departure and arrival, airport of departure and arrival, date of departure and arrival, border crossing point of entry into the territory of the State through which the passenger will enter the Republic of Latvia, the number of other aircraft passengers);

6) seat number of the person;

7) other aircraft passengers who should be considered contact persons within the scope of the particular flight (given name, surname, address, and contact information, seat number).

(3) The following shall be indicated in the request for the issuance of passenger data:

1) the given name, surname, and position of the official making the request. State intelligence and security services for which indication of the information referred to in this Clause would constitute a disclosure of an official secret shall indicate their name in the request;

2) justification of the need for passenger data;

3) the objective to be achieved;

4) the reason which precludes achievement of the objective or significantly hinders the achievement thereof if the passenger data is not to be issued;

5) information to be selected.

(4) The Passenger information unit shall refuse to issue the requested passenger data if the information referred to in Paragraph three of this Section has not been included in the request.

(5) The Passenger information unit shall issue the requested passenger data to the institution:

1) within 30 days from the day of receipt of the request referred to in Paragraph one of this Section;

2) as soon as possible, but not later than within 24 hours after the moment of receipt of the request referred to in Paragraph two of this Section.

(6) If the grounds to request and receive passenger data have ceased to exist, the institution which requested them shall immediately inform the Passenger information unit.

(7) If the grounds to request and receive passenger data have ceased to exist, the Passenger information unit shall immediately terminate issuance thereof to the relevant institution.

[*20 January 2022*]

**Chapter IV**

**Exchange of Passenger Data between Countries and International Organisations**

[*10 May 2018*]

**Section 15. Grounds for the Issuance of Passenger Data**

The Passenger information unit may issue passenger data from the Register to the Passenger information unit of a Member State, a third country, an international organisation or an agency thereof if there are grounds to believe that they may help the submitter of the request to prevent or detect a crime related to terrorism, a serious crime or to prevent threats to national security or public health. Passenger data may be issued from the Register upon a request of the competent authority of a foreign state or an international organisation or an agency thereof with the consent of a judge, except for the case referred to in Section 14, Paragraph one and Section 14.1, Paragraphs one and two of this Law.

[*10 May 2018; 20 January 2022*]

**Section 15.1 Exchange of Passenger Data between Member States and International Organisations**

(1) In order to receive passenger data from the Passenger information unit of a Member State, the institutions which have the right to request passenger data in order to meet the objectives referred to in Sections 10 and 15 of this Law shall address the Passenger information unit with a reasoned request.

(2) The Passenger information unit shall forward the received request to the Passenger information unit of the relevant Member State as soon as possible. The Passenger information unit shall communicate a reply of the Member State to the institution which has submitted the request within the shortest possible period of time.

(3) If immediate action is required to prevent a terrorist attack or a real threat to the life or health of a person, the competent institutions may address the Passenger information unit of the Member State with a reasoned request for the issuance of passenger data by concurrently sending a copy of the relevant request also to the national Passenger information unit.

(4) The Passenger information unit shall send information to Passenger information units of relevant Member States regarding compliance of the data individually processed in accordance with Section 9, Paragraph three of this Law if there are grounds to believe that such passenger data may help a Member State to prevent or detect crimes related to terrorism, serious crimes or to prevent a threat to national security.

(5) The conditions referred to in this Section for the exchange of data among Member States shall also be applicable to international organisations and agencies thereof.

(6) If Europol sends a request for the issuance of passenger data through the national unit of Latvia, it shall forward the relevant request to the Passenger information unit.

[*10 May 2018*]

**Section 15.2 Conditions for the Transfer of Passenger Data to Third Countries**

Passenger data may be transferred to a third country on a case-by-case basis, provided that:

1) general data protection requirements for the transfer of data to third countries are complied with;

2) transfer of data corresponds to the purpose specified in Section 15 of this Law;

3) a third country agrees to not transfer the data to another third country, except for the case when the transfer of data corresponds to the purpose specified in Section 15 of this Law and the consent of the Passenger information unit has been received for the transfer of data;

4) a third country undertakes to immediately, but not later than within 72 hours, inform the Passenger information unit of the transfer of data to another third country in cases where the transfer of data to another third country is necessary for the prevention of a terrorist act or a real threat to the life or health of a person and it is not possible to receive the consent of the Passenger information unit in time.

[*10 May 2018*]

**Section 16. Procedure for the Examination of a Request**

(1) After receipt of the request referred to in Section 15 of this Law, the Passenger information unit shall, within 30 days, evaluate the information and justification indicated in the request and refuse to issue the requested passenger data if the issuance thereof may:

1) jeopardise the national sovereignty and security of Latvia;

2) compromise the achievement of the objective of an operational activities procedure or criminal proceedings carried out in Latvia;

3) endanger the life, health or other legitimate interests of a person.

(11) If none of the reasons for refusal referred to in Paragraph one of this Section has been established and the request for passenger data does not concern the case referred to in Section 14.1, Paragraph one or two of this Law, the Passenger information unit shall, immediately, but not later than within three working days, submit the received request to a district (city) court for assessment according to the location of the institution.

(12) If the request concerns the case referred to in Section 14.1, Paragraph one or two of this Law, the Passenger information unit shall act in accordance with that specified in Section 14.1 of this Law.

(2) A judge shall ascertain that the information referred to in Section 11 of this Law is indicated in the request, evaluate the justification provided therein and decide on giving the consent to the issuance of data.

(3) In addition a judge shall evaluate the following circumstances and will not give the consent to the issuance of the requested passenger data if:

1) the issuance of the requested passenger data is clearly disproportionate with regard to the indicated objective or inappropriate for the achievement thereof;

2) the submitter of the request is not a competent subject in the field of the exchange of passenger data;

3) the issuance of passenger data fails to comply with the requirements for personal data protection with regard to the transfer of data to other states.

(4) If a judge lacks information which is necessary for deciding an issue of the consent, he or she shall ask the Passenger information unit to request additional information from the submitter of the request.

(5) A judge shall draw up the consent to the issuance of passenger data and also the refusal as a separate document or resolution. The decision of a judge may not be appealed.

(6) When issuing the requested passenger data from the Register the Passenger information unit shall comply with the time periods laid down in Section 13 of this Law. In urgent cases the Passenger information unit shall issue the requested passenger data from the Register in compliance with the conditions of Section 14 of this Law.

(7) If a judge has found that the issuance of passenger data from the Register as a matter of urgency is unjustified, the Passenger information unit shall immediately terminate the issuance thereof and also inform the submitter of the request by calling on it to immediately delete the received passenger data.

(8) The Passenger information unit shall immediately inform a data protection officer of the transfer of passenger data to a third country.

(9) If the Passenger information unit establishes the circumstances referred to in Paragraph one of this Section after initiation of the issuance of the requested passenger data, it may terminate the issuance of the relevant data and inform the submitter of the request thereof.

[*10 May 2018; 20 January 2022*]

**Section 17. Reply to a Request of a Foreign State or International Organisation**

A reply to a request of a competent institution of a foreign state or of an international organisation or agency thereof to issue passenger data from the Register shall be sent in the same way as the request was received. Information exchange shall take place in a language which is used in the relevant cooperation channel.

[*10 May 2018*]

**Section 18. Issuance of Passenger Data from the Register within the International Co-operation in the Field of Criminal Law**

A request to issue passenger data from the Register made within the international co-operation in the field of criminal law shall be examined in accordance with the requirements of laws and regulations governing international co-operation in the field of criminal law by taking into account the conditions for the issuance of passenger data laid down in this Law.

**Chapter V**

**Additional Requirements for Personal Data Protection**

**Section 19. Passenger Data Processing Requirements**

(1) The Passenger information unit shall process passenger data in accordance with the general requirements for personal data protection.

(2) It is prohibited to process passenger data that reveal race, ethnic or social origin, political opinions, religious or other beliefs, trade union membership, genetic peculiarities, information on the health, sex life or sexual orientation of a person, and also other special categories of personal data.

(3) If an air carrier has transferred for the inclusion in the Register passenger data which are not referred to in Section 4 of this Law and also information containing special categories of personal data, such data shall be automatically and permanently deleted immediately after receipt of the relevant information.

(4) The State Data Inspectorate shall, in accordance with the requirements of laws and regulations, perform supervision of the processing of personal data carried out by the Passenger information unit.

(5) If a personal data breach may pose a significant threat to the personal data protection or adversely affect the privacy of a data subject, the Passenger information unit shall immediately, but not later than within three working days, notify the data subject and the State Data Inspectorate of such breach.

[*10 May 2018*]

**Section 20. Obligation to Inform Passengers**

Air carriers shall ensure that the information on the transferring of data for the inclusion thereof in the Register shall be provided to passengers of aircrafts serviced by them in an easily accessible and understandable form.

**Section 21. Recording of Passenger Data Processing**

(1) Each processing of passenger data is accounted for in the Register.

(2) The Passenger information unit records requests for the issuance of passenger data and the given replies.

(3) The information on the recording of passenger data processing referred to in Paragraphs one and two of this Section shall be retained for five years.

**Section 22. Data Protection Officer**

(1) A data protection officer shall be an official assigned by the State Security Service who is responsible for the supervision of the processing of personal data of passengers and the implementation of data protection measures.

(2) A data protection officer shall meet the requirements for such specialist laid down in the general framework of the protection of data of natural persons.

(3) For the purpose of carrying out the tasks specified in this Law, a data protection officer has the right to access the passenger data processed in the Register and the information regarding activities conducted in the Register.

(4) If there are grounds to believe that the processing of passenger data has been unlawful, a data protection officer may report it to the State Data Inspectorate.

(5) As to the issues related to the processing of his or her personal data in the Register, a data subject may only contact a data protection officer.

[*10 May 2018; 24 October 2019*]

**Chapter VI**

**Administrative Offences in the Processing of Aircraft Passenger Data and Competence in Administrative Offence Proceedings**

[*24 October 2019 / Chapter shall come into force on 1 July 2020. See Paragraph 2 of Transitional Provisions*]

**Section 23. Failure to Transfer Passenger Data and Transfer of Incomplete or Incorrect Data**

For the failure to transfer aircraft passenger data, transfer of incomplete or incorrect data laid down in the laws and regulations to the Passenger information unit for the automated inclusion thereof in the Register, a fine from six hundred and twenty to one thousand and twenty units of fine shall be imposed on the carrier – legal person.

[*24 October 2019 / Section shall come into force on 1 July 2020. See Paragraph 2 of Transitional Provisions*]

**Section 24. Competence in Administrative Offence Proceedings**

The administrative offence proceedings for the violations referred to in Section 23 of this Law shall be conducted by the State Police.

[*24 October 2019 / Section shall come into force on 1 July 2020. See Paragraph 2 of Transitional Provisions*]

**Transitional Provisions**

[*24 October 2019*]

1. Air carriers shall start to fulfil the obligation laid down in Section 5 of this Law to transfer passenger data for the inclusion thereof in the Register not later than on 1 September 2017.

[*24 October 2019*]

2. Chapter VI of the Law shall come into force concurrently with the Law on Administrative Liability.

[*24 October 2019*]

3. The condition provided for in Section 5, Paragraph one of this Law regarding the transfer of passenger data on intra-EU flights for the automated inclusion thereof in the Register shall be applicable to an air carrier not later than from 1 July 2020. Until the abovementioned data an air carrier shall transfer the passenger data on intra-EU flights to the Passenger information unit, provided that its request has been received to provide passenger data on a specific route.

[*24 October 2019*]

**Informative Reference to European Union Directive**

[*10 May 2018*]

The Law contains legal norms arising from Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

Aircraft Passenger Data Processing Law

**Annex**

[*10 May 2018*]

**Criminal Offences for the Prevention and Detection of which it is Acceptable to Process the Passenger Data:**

1) participation in a criminal organisation;

2) trafficking in human beings;

3) sexual exploitation of children and child pornography;

4) illicit trafficking in narcotic drugs and psychotropic substances;

5) illicit trafficking in weapons, ammunition, and explosives;

6) corruption;

7) fraud, including that which affects financial interests of the European Union;

8) laundering of the proceeds from crime and counterfeiting of currency, including EUR;

9) computer-related crime and cybercrime;

10) environmental crime, including illicit trafficking in endangered animal species and in endangered plant species and varieties;

11) facilitation of unauthorised entry and residence;

12) murder or committing of grievous bodily injury;

13) illicit trade in human organs and tissue;

14) kidnapping, illegal restraint and hostage taking;

15) organised and armed robbery;

16) illicit trafficking in cultural goods, including antiques and works of art;

17) counterfeiting and piracy of products;

18) forgery of administrative documents and trafficking therein;

19) illicit trafficking in hormonal substances and other growth promoters;

20) illicit trafficking in nuclear or radioactive materials;

21) rape;

22) crimes within the jurisdiction of the International Criminal Court;

23) unlawful seizure of aircraft or ships;

24) sabotage;

25) trafficking in stolen vehicles;

26) industrial espionage.

The Law shall come into force on 3 April 2017.

The Law has been adopted by the *Saeima* on 19 January 2017.

President R. Vējonis

Rīga, 7 February 2017