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

12 September 2013 [shall come into force on 10 October 2013];

22 June 2017 [shall come into force on 19 July 2017].

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:

**Biometric Data Processing System Law**

**Chapter I. General Provisions**

**Section 1.**The following terms are used in this Law:

1) **biometric data**– a set of physical properties and indicators of a natural person [digital picture of a face, finger (palm) trails or prints];

2) **biometric data processing**– any operations with biometric data including data acquisition, registration, storage, sorting, modification, use, comparison, transfer, transmission, disclosure, blocking or deletion;

3) **identity**– a set of natural person’s data, physical properties and indicators which allow to clearly distinguish such person from another natural person;

4) **finger (palm) prints**– prints obtained from a person’s hand fingers (palm);

5) **finger (palm) trails**– reflection of a person’s hand finger (palm) which is left on an object surface by a person when touching or grasping the object;

6) [12 September 2013].

[*12 September 2013*]

**Section 2.**The purpose of this Law is to ensure the creation of a unified biometric data processing system to make it possible to establish identity of natural persons, and also to prevent the use of another person’s identity.

**Chapter II. Creation of the Biometric Data Processing System, Entry of Biometric Data, Updating and Storage Thereof**

**Section 3.**The Biometric Data Processing System is a State Information System the manager and holder of which is the Information Centre of the Ministry of the Interior.

**Section 4.**The creation, maintenance and improvement of the Biometric Data Processing System shall be financed from the funds intended for such purposes in the State budget.

**Section 5.**The data obtained from the following sources shall be included in the Biometric Data Processing System:

1) when issuing personal identification documents;

2) [12 September 2013];

3) [12 September 2013];

4) when issuing seafarer identification documents;

5) when issuing drivers’ licences;

6) [12 September 2013];

7) [12 September 2013];

8) [12 September 2013];

9) from non-identified bodies;

10) as a result of operational activities, counter-intelligence and intelligence measures. The obtained data shall be included in the Biometric Data Processing System if threats to national security and public order need to be prevented, and if the decision to enter such data is taken by the body performing operational activities who has obtained the relevant data;

11) as a result of investigative actions and from detained, suspected, accused and convicted persons;

12) from the persons who does not have a valid personal identification documents after establishing such fact.

[*12 September 2013*]

**Section 6.**In the cases provided for in Section 5, Clauses 1, 4, 5 and 12 of this Law, the following data shall be included in the Biometric Data Processing System:

1) on persons who are registered with the Population Register:

a) digital picture of the face;

b) digital picture of finger (palm) trails (if it can be obtained);

c) the given name (names) and surname;

d) personal identity number;

e) gender;

f) nationality and type thereof;

g) fact of the death of the person;

h) institution – acquirer of the biometric data;

i) justification for obtaining the biometric data;

j) date of obtaining the biometric data;

2) on persons who are not registered with the Population Register:

a) digital picture of the face;

b) digital picture of finger (palm) trails (if it can be obtained);

c) the given name (names) and surname;

d) date of birth of the person;

e) nationality and type thereof;

f) gender;

g) institution – acquirer of the biometric data;

h) justification for obtaining the biometric data,

i) date of obtaining the biometric data.

[*12 September 2013*]

**Section 7.**(1) In the cases provided for in Section 5, Clauses 10 and 11 of this Law, the following data shall be included in the Biometric Data Processing System on a person from which finger (palm) prints have been obtained:

1) digital picture of the face;

2) digital picture of the finger (palm) prints;

3) the given name (names), surname of the person;

4) date of birth of the person;

5) the personal identify number (if such has been assigned);

6) nationality and type thereof;

7) gender;

8) legal qualification of a criminal offence or administrative offence (if such has been found);

9) justification for obtaining the biometric data [finger (palm) prints];

10) institution – acquirer of the biometric data;

11) date of obtaining the biometric data;

12) registration number in the event records or the number of the investigatory records case or criminal case.

(2) If a person has changed the given name or surname, the previous given name and surname shall also be indicated.

**Section 8.**In the cases provided for in Section 5, Clauses 10 and 11 of this Law, the following data shall be included in the Biometric Data Processing System on finger (palm) trails of persons:

1) digital picture of the finger (palm) trails;

2) registration number in the event records or the number of the investigatory records case or criminal case;

3) date of the event;

4) address of the event;

5) legal qualification of a criminal offence or administrative offence (if such has been found);

6) institution – acquirer of the biometric data;

7) date of obtaining the biometric data.

**Section 9.**The following data shall be included in the Biometric Data Processing System on a non-identified body:

1) digital picture of the face (if such can be obtained);

2) digital picture of finger (palm) prints (if such can be obtained);

3) registration number in the event records or the number of the investigatory records case or criminal case;

4) the date when the non-identified body was found;

5) the address or geographic co-ordinates of the place where the non-identified body was found;

6) institution – acquirer of the biometric data;

7) date of obtaining the biometric data.

**Section 10.**(1) Inclusion and updating of the data referred to in Sections 6, 7, 8 and 9 of this Law in the Biometric Data Processing System shall be ensured by:

1) the State Police;

2) the Financial Police;

3) the Military Police;

4) the Prison Administration;

5) the Corruption Prevention and Combating Bureau;

6) customs authorities;

7) the State Border Guard;

8) the State security institutions;

9) the Road Traffic Safety Directorate;

10) the Maritime Administration of Latvia;

11) the Office of Citizenship and Migration Affairs;

12) the Internal Security Office.

(2) The institutions referred to in Paragraph one of this Section shall be responsible for the correct entry of biometric data in the Biometric Data Processing System, and also for updating the entered data during the storage thereof.

(3) The Cabinet shall determine procedures by which and amount in which the institutions referred to in Paragraph one of this Section shall enter and update data in the Biometric Data Processing System, and also conditions for the performance of the abovementioned activities.

[*12 September 2013; 22 June 2017*]

**Section 11.**(1) The data obtained in the cases provided for in Section 5, Clauses 1, 4, 5 and 11 of this Law (except for the data obtained as a result of investigative actions) shall be stored in the Biometric Data Processing System:

1) for 10 years after the death of the person if the fact of death of the person is registered with the Population Register;

2) 75 year after the day of the first entry if the person is not registered with the Population Register.

(2) The data obtained in the case provided for in Section 5, Clause 9 of this Law shall be stored in the Biometric Data Processing System for five years after its entry.

(3) The data obtained in the cases provided for in Section 5, Clause 10 of this Law shall be deleted by the body performing operational activities which has obtained such data, as soon as the necessity to keep them has ceased to exist. Within a year after entering the data in the Biometric Data Processing System, the body performing operational activities which has obtained such data shall evaluate the usefulness of its further storage and, where necessary, take the decision to extend the time period for data storage for a year. The body performing operational activities shall decide on each next extension of the time period for data storage within a year after taking the previous decision. If such decision is not taken, data shall be automatically deleted.

(4) Data obtained as a result of the investigative actions shall be stored in the Biometric Data Processing System for 75 years after their entry or deleted at the moment when the identity of the data owner is established.

(5) The data obtained in the case provided for in Section 5, Clause 12 of this Law shall be stored in the Biometric Data Processing System until the moment when a person receives a personal identification document, or the time periods laid down in Paragraph one of this Section shall be complied with if a person does not receive a personal identification document during his or her life.

(6) The procedures for the destruction of biometric data shall be determined by the Cabinet.

[*12 September 2013*]

**Chapter III. Use and Monitoring of Biometric Data**

**Section 12.**The data entered in the Biometric Data Processing System shall be restricted access information.

**Section 13.**The data entered in the Biometric Data Processing System shall be used to ensure:

1) prevention of the use of another person’s identity;

2) verification of the identity of the person in the process of issuing personal identification documents, and also in the process of issuing other documents referred to in this Law or establishment of the person’s identity in the process of issuing personal identification documents;

3) establishment of the identity of the person during intelligence, counter-intelligence, operational activities, and also during analysis of the obtained information;

4) prevention of criminal offences and other violations of the law;

5) detection of criminal offences and search for the persons who have committed a criminal offence;

6) verification of the identity of detained, suspected, accused and convicted persons;

7) verification of the identity of the person when carrying out border check of persons;

8) verification of the identity of the person when carrying out the control of conditions for the stay of foreigners;

9) verification of the identity of asylum seekers;

10) biometric identification of non-identified bodies (comparison of a sample with all biometric data samples entered in the Biometric Data Processing System to match it with one of the biometric data samples entered in the Biometric Data Processing System and, if such match is established, to establish the identity of the owner of the sample to be compared);

11) search for missing persons;

12) verification of the identity of the person, when providing a public service to the person, for the provision of which the identity of the person needs to be verified in accordance with the requirements of the laws and regulations. The verification referred to in this Paragraph where the data of the person whom the service is being provided is compared with the data of this person already accumulated in the Biometric Data Processing System shall be carried out only with the consent of the person;

13) establishment of the identity of the person if it is necessary for the provision of emergency medical care.

[*12 September 2013*]

**Section 14.**(1) The following institutions are entitled to use the Biometric Data Processing System for the performance of the functions referred to in Section 13 of this Law:

1) the State Police;

2) the Financial Police;

3) the Military Police;

4) the Prison Administration;

5) the Corruption Prevention and Combating Bureau;

6) customs authorities;

7) the State Border Guard;

8) the State security institutions;

9) the Ministry of Foreign Affairs;

10) the Road Traffic Safety Directorate;

11) the Maritime Administration of Latvia;

12) the Office of Citizenship and Migration Affairs;

13) the Prosecutor’s Office;

14) court;

15) the Information Centre of the Ministry of the Interior;

16) in-patient medical treatment institutions entered in the Register of Medical Treatment Institutions which ensure provision of emergency medical care;

17) municipal police;

171) the Internal Security Office;

18) other State and local government institutions if an external legal act provides for the use of the Biometric Data Processing System.

(2) The Cabinet shall determine procedures by which and amount in which the institutions referred to in Paragraph one of this Section shall use the data entered in the Biometric Data Processing System.

[*12 September 2013; 22 June 2017*]

**Section 15.**Provision of the data entered in the Biometric Data Processing System to foreign competent authorities shall be permissible in compliance with the international agreements binding on the Republic of Latvia and legal acts of the European Union.

**Section 16.**Compliance with this Law shall be supervised by the Data State Inspectorate in accordance with the procedures laid down in the laws and regulations regarding personal data protection.

**Transitional Provisions**

1. With the coming into force of this Law, the Biometric Data Processing Law adopted on 31 May 2007 (*Latvijas Republikas Saeimas un Ministru Kabineta Ziņotājs*, 2007, No. 13) is repealed.

2. The Cabinet shall, by 31 December 2009, issue the Cabinet regulations provided for in Section 10, Paragraph one, Section 11, Paragraph three and Section 14, Paragraphs one and four of this Law.

3. The institutions referred to in this Law, except for the Maritime Administration of Latvia, shall ensure biometric data processing in accordance with the procedures laid down in the Law starting from 1 January 2011.

4. The Maritime Administration of Latvia shall ensure biometric data processing in accordance with the procedures laid down in this Law after ratification of the Seafarers’ Identity Documents Convention of the International Labour Organisation of 19 June 2003, but no earlier than from 1 January 2011.

5. The Cabinet shall, by 31 December 2013, issue the regulations referred to in Section 10, Paragraph three, Section 11, Paragraph six and Section, Paragraph two of this Law. Until the day when the respective Cabinet regulations come into force but no longer than until 31 December 2013, the Cabinet Regulation No. 233 of 3 April 2012, Regulations Regarding Biometric Data Processing System, shall be in force, insofar as it is not in contradiction with this Law.

[*12 September 2013*]

This Law has been adopted by the *Saeima* on 21 May 2009.

President V. Zatlers

Riga, 10 June 2009