The *Saeima* 1 has adopted and

the President has proclaimed the following law:

**On Processing of Personal Data in the Criminal Proceedings and Administrative Offence Proceedings**

**Chapter I**

**General Provisions**

**Section 1. Terms Used in this Law**

The following terms are used in this Law:

1) **processor** – a natural person or legal person, public authority, derived public person or body thereof which processes personal data on behalf of the controller in conformity with that laid down in laws and regulations;

2) **biometric data** – personal data after specific technical processing which apply to the physical, physiological or behavioural characteristics of a natural person and which allow or confirm the unique identification of that natural person;

3) **data subject** – an identified or identifiable natural person;

4) **genetic data** – personal data which apply to the inherited or acquired genetic characteristics of a natural person, provide unique information on the physiology or the health of such natural person and arise from an analysis of a biological sample of such natural person;

5) **filing system** – any structured set of personal data which is accessible in accordance with specific criteria regardless of whether such set of data is centralised, decentralised or dispersed;

6) **competent authority** – a public authority, derived public person or body thereof the competence of which includes the prevention, investigation or detection of criminal offences or administrative offences, the application or enforcement of criminal penalties or administrative penalties or the performance of other activities related to administrative offence proceedings or criminal proceedings;

7) **controller** – a legal person, public authority, derived public person or body thereof which, alone or jointly with other institutions, determines the purposes and means of the processing of personal data;

8) **joint controllers** – two or several controllers which jointly determine the purposes and means of the processing of personal data;

9) **personal data** – any information which applies to a data subject;

10) **personal data breach** – a breach of security which results in accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed;

11) **processing of personal data** – any operation which is performed with personal data regardless of the type of the processing of personal data, for example, collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making them available, alignment or combination, restriction, erasure or destruction thereof;

12) **restriction of the processing of personal data** – marking, distinction of personal data from other personal data or other similar operations for the purpose of restricting the processing of specific personal data in the future;

13) **profiling** – any form of automated processing of personal data manifested as the use of personal data to evaluate certain personal aspects related to a natural person, in particular to analyse or predict the performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movement of such natural person;

14) **pseudonymisation** – a set of operations which ensure the processing of personal data in such a manner that the natural person is not identifiable without additional information which is kept separately and which is subject to the relevant technical and organisational measures to ensure that the natural person is not identifiable without such information;

15) **recipient** – a natural person or legal person, public authority, derived public person or body thereof to which the personal data are disclosed. A public authority, derived public person or body thereof which receives personal data in relation to the specific investigation in criminal proceedings or administrative offence proceedings shall not be regarded as a recipient;

16) **international organisation** – an organisation and its subordinate bodies which are governed by public international law, or any other body which is established by or on the basis of an international agreement entered into by two or several countries;

17) **third country** – a country other than a Member State of the European Union or the European Economic Area;

18) **data concerning health** – personal data related to the physical or mental health of a natural person, including the receipt of health care services, and which provide information on his or her health condition.

**Section 2. Purpose of this Law**

The purpose of this Law is to protect the fundamental rights of natural persons, in particular the inviolability of private life, during the processing of personal data by competent authorities in order to:

1) prevent, investigate and detect criminal offences and administrative offences;

2) apply and enforce criminal penalties and administrative penalties;

3) perform other activities related to administrative offence proceedings or criminal proceedings, including to apply procedural compulsory measures, to ensure monitoring of such persons who are conditionally released from criminal liability, proceedings regarding criminally acquired property, proceedings regarding compulsory measures of a medical nature, proceedings regarding compulsory measures of a correctional nature, proceedings regarding coercive measures for legal persons, proceedings regarding the course of examination *de novo* of valid rulings and enforcement of decisions taken within the scope thereof.

**Section 3. Scope of Application and Exceptions of Application of the Law**

(1) This Law shall be applied to the processing of personal data which is performed by a competent authority for the purposes referred to in Section 2 of this Law if processing is fully or partly performed by automated means or personal data to be processed form a filing system or are intended to form part of a filing system.

(2) In compliance with Paragraph one of this Section, this Law shall be also applied to such processing of personal data that is performed by the Office of the Prosecutor, when fulfilling the functions for the protection of the rights and lawful interests of persons and the State laid down in the Office of the Prosecutor Law for the achievement of the purpose laid down in Section 2 of this Law.

(3) This Law shall not be applied to the processing of personal data that is performed by a competent authority for purposes other than referred to in Section 2 of this Law. 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) (hereinafter – the Data Regulation) shall be applied to such processing of personal data, insofar as the Data Regulation applies to the processing of such personal data.

**Chapter II**

**General Provisions for the Processing of Personal Data**

**Section 4. General Principles for the Processing of Personal Data**

(1) Personal data shall be:

1) processed lawfully and fairly;

2) collected for specified, explicit and legitimate purposes, and not processed in a manner that is incompatible with the abovementioned purposes;

3) processed so that they would conform to the purpose for the processing of personal data laid down in Section 2 of this Law and would not be excessive, having regard to the purpose for which they are processed;

4) processed so that they would be accurate and up to date. The controller shall ensure that inaccurate personal data, having regard to the purpose for which they are processed, are erased or rectified without delay;

5) kept in a form which permits identification of data subjects for no longer than it is necessary for the purposes of the processing of personal data;

6) processed by using appropriate technical or organisational measures in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

(2) The processing of personal data by the same or another controller for the purpose other than intended initially may be performed if:

1) the processing of personal data is performed for the purposes referred to in Section 2 of this Law, is necessary for the performance of tasks laid down in external laws and regulations, and is commensurate with the purpose other than intended initially;

2) the processing of personal data is regarded as archiving in the public interest, scientific, statistical or historical use for the purposes referred to in Section 2 of this Law and the appropriate right of a data subject to the protection of own personal data is ensured.

(3) If personal data are included in the documents of short-term, long-term or permanent storage, they are subject to complete or partial erasure after agreement of the deed on document destruction with the National Archives of Latvia in accordance with the procedures laid down in external laws and regulations. A document of short-term storage may be destroyed (complete or partial erasure of personal data) without such agreement only if the storage period of the respective type of document has been agreed with the National Archives of Latvia and such period has expired.

(4) The controller is responsible for the conformity of the processing of personal data with the requirements of this Section and it must be able to demonstrate such conformity.

**Section 5. Lawfulness of the Processing of Personal Data**

The processing of personal data shall be regarded to be lawful insofar such processing is necessary for the performance of a task carried out by a competent authority for the purposes referred to in Section 2 of this Law and that is determined by an external law or regulation governing the activity of the competent authority.

**Section 6. Distinction of Personal Data and Verification of Quality**

(1) The controller shall, when processing personal data, make a clear distinction of the personal data of various categories of data subjects, and also personal data which are based on facts from personal data which are based on personal assessments.

(2) The controller shall ensure that personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made otherwise available. A competent authority shall, prior to transmitting personal data, verify whether personal data are accurate, complete, reliable and up to date. When transmitting personal data, the controller shall add necessary information which allows a competent authority to assess whether the data are accurate, complete, reliable and up to date.

(3) If incorrect personal data have been transmitted or personal data have been unlawfully transmitted, the recipient shall be notified thereof without delay. In such case the personal data shall be rectified or erased, or processing thereof shall be restricted in accordance with Section 13 of this Law.

**Section 7. Specific Conditions for the Processing of Personal Data**

(1) A competent authority shall, upon transferring personal data, inform the recipient of the specific requirements for the processing of personal data laid down in laws and regulations that must be complied with by the competent authority and also of the obligation of the recipient to comply with these requirements.

(2) The provisions of Paragraph one of this Section shall also apply to recipients in other Member States of the European Union, European Economic Area or agencies, offices and structures established in compliance with Title V, Chapters 4 and 5 of the Treaty on the Functioning of the European Union.

**Section 8. Processing of Special Categories of Personal Data**

The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership of a natural person, and also the processing of genetic data and biometric data for the purpose of uniquely identifying a natural person, or the processing of data concerning a natural person’s health or sex life, or his or her sexual orientation shall be allowed only if such processing has been laid down in the relevant law or is absolutely necessary and if safeguards for the rights of a data subject apply to such processing and at least one of the following conditions has set in:

1) the processing of personal data is necessary to protect the vital interests of the data subject or of another natural person;

2) such personal data are processed which have been made public by the data subject himself or herself.

**Section 9. Automated Individual Decision-making**

(1) A competent authority is prohibited from making such decisions that are based solely on automated processing, including profiling, if they produce an adverse legal effect on a data subject or significantly affect him or her, except for cases where such decision-making is provided for in an external law or regulation which includes safeguards for the rights of a data subject.

(2) Profiling which discriminates against a natural person on the basis of special categories of personal data referred to in Section 8 of this Law shall be prohibited.

**Chapter III**

**Rights of a Data Subject**

**Section 10. Procedures for Exercising the Rights of a Data Subject**

(1) A data subject has the right to submit to the controller a request in respect of the processing of his or her personal data and to receive a reply from the controller by indicating further actions in relation to the request, without undue delay, but not later than within a month after the day of receipt of the request. If a data subject has not specified otherwise and it is technically possible, the controller shall reply in the same form as the request was submitted.

(2) A data subject shall exercise his or her rights laid down in this Law free of charge. The controller has the right to charge a fee for executing the request in conformity with laws and regulations regarding paid services for the provision of information if the request of the data subject is excessive or repeats regularly. The controller shall inform the data subject of the reasons for charging a fee.

(3) If the request of the data subject is unjustified, the controller shall refuse to execute the request included therein. The controller shall provide grounds for considering the request unjustified.

(4) If the controller has reasonable doubts concerning the identity of the natural person who submits the request, it may request the provision of additional information necessary to confirm the identity of the data subject.

(5) The data subject has the right to contest and appeal the actions of the controller or processor in relation to his or her request in accordance with the procedures laid down in the Administrative Procedure Law, but the actions of a supervisory authority (hereinafter – the Data State Inspectorate) – in accordance with the procedures laid down in the Personal Data Processing Law. If personal data are processed within the scope of operational activities, criminal proceedings or administrative offence proceedings, complaints regarding the processing of personal data shall be examined in accordance with the procedures laid down in the laws and regulations governing operational activities, criminal proceedings or administrative offence proceedings.

**Section 11. Informing of a Data Subject**

(1) The controller shall make available at least the following information to a data subject:

1) the name and contact details of the controller;

2) the contact details of the data protection officer;

3) the purpose of the personal data processing;

4) information on the right to lodge a complaint to the Data State Inspectorate and contact details of the Data State Inspectorate;

5) information on the right to request the controller to ensure access to personal data for the data subject, rectify or erase them, or restrict the processing of the personal data of the data subject.

(2) The controller shall provide at least the following information to a data subject in accordance with the procedures laid down in external laws and regulations for the protection of the rights and legitimate interests of the data subject:

1) the legal basis for the processing of personal data;

2) the time period for the storage of personal data, or, if not possible, the criteria used to determine the time period;

3) the categories of recipients, also in third countries or international organisations.

(3) The controller shall provide the information on the rights of the data subject in a concise, intelligible and easily accessible form using clear and plain language.

(4) The processing of personal data, without informing the data subject, shall be performed in the cases laid down in external laws and regulations.

**Section 12. Right of Access by a Data Subject**

(1) A data subject has the right to receive from the controller information on whether or not his or her personal data are being processed within a reasonable time period, however not later than within a month, and also to obtain the following information:

1) the purpose of and legal basis for the processing of personal data;

2) the categories of the processed personal data;

3) the recipients or categories of recipients;

4) the time period for the storage of personal data, or, if not possible, the criteria used to determine the time period;

5) information on the right to request from the controller to rectify or erase the personal data of a data subject, or restrict processing thereof;

6) information on the right to lodge a complaint to the Data State Inspectorate and contact details of the Data State Inspectorate;

7) information on the processed personal data and any available information on their origin.

(2) Paragraph one of this Section shall not be applied if the law which governs the processing of the particular personal data provides for other procedures for exercising the right of access of the data subject. In such case, the controller shall, without undue delay, not later than within a month, inform the data subject in writing on the refusal or restrictions to access his or her personal data and on the reasons for the refusal or restrictions. Such information may be omitted if the law which governs the processing of particular personal data provides for that the data subject shall not be informed on the refusal or restrictions to access his or her personal data or on the reasons for the refusal or restrictions. The controller shall inform the data subject on the right to lodge a complaint to the Data State Inspectorate or apply to a court.

(3) The controller shall ensure the possibility to the Data State Inspectorate, upon its request, to familiarise with the decision made on the basis of Paragraph two of this Section and information on the basis of which such decision was made.

**Section 13. Right to Request Rectification, Erasure of Personal Data or Restriction of the Processing of Personal Data**

(1) The data subject has the right to request from the controller without undue delay, however not later than within a month after the day of the receipt of the request, to supplement or rectify his or her personal data which are inaccurate or incomplete.

(2) The data subject has the right to request from the controller without undue delay, however not later than within a month after the day of the receipt of the request, to erase his or her personal data if the requirements of Section 4, 5 or 8 of this Law are infringed during the processing of personal data.

(3) The controller shall not erase personal data, but shall restrict the processing thereof in the following cases:

1) the data subject contests the accuracy of his or her personal data, but it is not possible to ascertain the accuracy or inaccuracy thereof. In such case the controller shall inform the data subject before revocation of the restriction of the processing of personal data;

2) it is necessary to maintain the personal data for the purposes of evidence.

(4) The controller shall not inform the data subject on any refusal to rectify his or her personal data, to erase or restrict the processing thereof and on the reasons for refusal if the law which governs the processing of the particular personal data provides for the processing of personal data without informing the data subject.

(5) If the inaccurate personal data are received from a competent authority, the controller shall inform the competent authority on the rectification of personal data.

(6) If the controller rectifies or erases personal data or restricts the processing thereof, the controller shall notify the recipients thereof and the recipients shall rectify, erase the relevant personal data or restrict the processing thereof.

**Section 14. Exercising the Rights of a Data Subject Through the Data State Inspectorate**

(1) In the cases referred to in Section 11, Paragraph four, Section 12, Paragraph two and Section 13, Paragraph four of this Law, a data subject has the right to submit a request to the Data State Inspectorate regarding the processing of his or her personal data or inspection of the processing thereof.

(2) If the data subject has submitted the request referred to in Paragraph one of this Section to the controller, the controller shall, within seven working days from the day of the receipt of the request, forward it to the Data State Inspectorate by informing the data subject thereof.

(3) After performance of the necessary inspections, the Data State Inspectorate shall inform the data subject at least on the performance of all necessary inspections, and also on his or her rights to appeal the actions of the Data State Inspectorate to a court.

**Chapter IV**

**Controller, Processor and Data Protection Officer**

**Section 15. General Obligations of the Controller**

(1) Taking into account the nature, scope, context and purpose of the processing of personal data and also various risks related to the processing of personal data in respect of the rights of the data subject, the controller shall implement appropriate technical and organisational measures, including pseudonymisation, use logical and physical protection measures in order to ensure that the processing of personal data is performed in accordance with the requirements of this Law and conforms with the principles of the processing of personal data.

(2) The controller has the obligation to review and update technical and organisational measures on a regular basis.

(3) The employees of the controller and other persons under the subordination of the controller shall process personal data only in conformity with laws and regulations and in accordance with the instructions of the controller.

(4) Joint controllers shall agree in writing on measures to be taken for the fulfilment of the requirements of this Law, including the procedures for exercising the rights of the data subject, insofar they already do not arise from external laws and regulations.

**Section 16. Processor and Actions Entrusted Thereto**

(1) The controller may entrust the processing of personal data to the processor which provides sufficient guarantees to implement appropriate technical and organisational measures, and also to ensure the protection of the rights of the data subject.

(2) The controller shall entrust the processing of personal data to the processor by entering into a written agreement which includes the information on the personal data to be processed, duration, nature and purpose of the processing of personal data, categories of personal data and data subjects, obligations and rights of the controller, conditions for the involvement of another processor, and also such provisions that the processor shall:

1) act only in accordance with the instructions of the controller;

2) ensure that persons who are authorised to process the personal data have committed themselves to ensure confidentiality;

3) assist the controller by appropriate means to ensure conformity with the requirements laid down in this Law;

4) erase or transfer (at the choice of the controller) all personal data related to the relevant processing after completing the processing of personal data. The processor shall not erase personal data if external laws and regulations provide for the storage thereof;

5) provide all necessary information to the controller to demonstrate that the processor complies with all obligations laid down in this Section.

(3) The processor, its employees and other persons under the subordination of the processor shall process personal data only in conformity with laws and regulations and in accordance with the instructions of the controller.

(4) The processor is allowed to involve another processor only with the written consent of the controller. If the controller agrees to the involvement of another not specifically stated processor, the processor shall, prior to the involvement or change of another processor, inform the controller thereof. The controller has the right to object to the particular processor.

(5) If the processor is laid down in a law or regulation and it does not contain the information and provisions referred to in Paragraph two of this Section, the controller shall agree with the processor thereon in writing.

**Section 17. Prohibition to Disclose Information**

The employees of the controller or the processor and other persons under the subordination thereof are prohibited from disclosure of information (except for publicly accessible information) which has been obtained in relation to the processing of personal data. This prohibition shall also be valid after termination of service or employment relationships or other relationships laid down in the contract.

**Section 18. Registration of Processing Operations**

(1) The controller shall compile and maintain the following information on the personal data processing operations for which it is responsible:

1) the name and contact details of the controller or all joint controllers;

2) the given name, surname (for a legal person – the name and registration number) and contact details of the data protection officer;

3) the purposes of the processing of personal data;

4) the legal basis for the processing of personal data;

5) the categories of such recipients to whom personal data are disclosed or to whom they will be disclosed, including recipients in third countries or international organisations;

6) the categories of data subjects and description thereof, including categories which include transfers of personal data to a third country or international organisation;

7) information on profiling if such is used;

8) if possible – the time period after which personal data will be erased by specifying this in respect of the particular category of personal data;

9) technical and organisational measures ensuring the protection of personal data.

(2) The processor shall establish and maintain a register for the personal data processing operations performed on behalf of the controller, including at least the following information therein:

1) the given name, surname (for a legal person – the name and registration number) and contact details of the processor or processors, and also that of the controller on behalf of which the processor operates;

2) the given name, surname and contact details of the data protection officer;

3) the categories of the personal data processed on behalf of the controller;

4) information on the transfer of personal data to a third country or international organisation;

5) the general description of such technical and organisational measures which ensure a level of security appropriate to the risk of the rights and legitimate interests of the data subject.

(3) The information referred to in this Section shall be provided to the Data State Inspectorate upon the request and free of charge.

**Section 19. Performance of Audit Trails**

(1) The controller shall ensure the performance of audit trails at least of the following operations in automated processing systems: collection, consultation, alteration, disclosure including transfers, combination or erasure. Trails of consultation and disclosure should be formed in a way to ensure the possibility to ascertain the reason for the relevant operations, the date and time and, insofar as it is possible, to identify the person who consulted or disclosed personal data, and also the recipients of such personal data.

(2) Audit trails shall be used in order to verify lawfulness of the processing of personal data, to perform self-monitoring, to ensure the integrity and security of the personal data, and also for the needs of criminal proceedings, administrative offence proceedings, departmental examination, operational activities measures, application of criminal penalties, administrative penalties, compulsory measures of a correctional nature, compulsory measures of a medical nature, procedural compulsory measures and for the needs of the monitoring process of persons conditionally released from criminal liability.

(3) The controller and processor shall make audit trails available to the Data State Inspectorate upon request and free of charge.

**Section 20. Cooperation with the Data State Inspectorate**

The controller and processor shall cooperate with the Data State Inspectorate in the performance of its tasks and upon request of the Data State Inspectorate shall provide information necessary for the performance of certain tasks so that it could ascertain about conformity of the processing of personal data with the requirements of this Law.

**Section 21. Data Protection Impact Assessment**

(1) If the type of the processing of personal data, in particular, by using new technologies, and taking into account the nature, scope, context and purposes of the processing, could result in the risks to the rights and legitimate interests of the data subject, the controller shall, prior to the processing of personal data, assess the impact of the envisaged processing operations on the protection of personal data.

(2) The assessment shall contain at least a general description of the envisaged personal data processing operations, an assessment of the risks to the rights and legitimate interests of data subjects, the measures intended to prevent the abovementioned risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate conformity with this Law, and the rights and legitimate interests of data subjects and other relevant persons are taken into account.

**Section 22. Requesting of the Opinion of the Data State Inspectorate on the Processing of Personal Data**

(1) Prior to the processing of personal data which will be included in the information system, the controller or processor shall consult the Data State Inspectorate in any of the following cases:

1) it is determined in the data protection impact assessment that the processing of personal data may result in a high risk to the rights and legitimate interests of the data subject if the controller fails to implement the measures for minimising the risk;

2) the type of the processing of personal data, in particular, using new technologies, mechanisms or procedures, is related to a high risk to the rights and legitimate interests of data subjects.

(2) The Data State Inspectorate shall provide an opinion on the impact of the processing of personal data on data protection within six weeks after receipt of the request. Taking into account the complexity of the envisaged processing, the time period may be extended by one month by informing the controller or processor accordingly thereof.

(3) The Data State Inspectorate may establish a list of the personal data processing operations which are subject to prior consultation in accordance with Paragraph one of this Section.

**Section 23. Notification of a Personal Data Breach to the Data State Inspectorate**

(1) In the event of a personal data breach, the controller shall notify the Data State Inspectorate thereof immediately, however not later than within 72 hours after having become aware of the breach. If the controller has not complied with the specified period, upon notifying the Data State Inspectorate of a personal data breach, it shall also inform of the reasons for exceeding the time period.

(2) The processor, as soon as it has become aware of a personal data breach, shall notify the controller thereof immediately.

(3) The notification referred to in Paragraph one of this Section shall contain at least the following information:

1) the nature of the personal data breach, including the categories of the relevant data subjects and the approximate number of the categories of data subjects, and also the categories of the relevant personal data and the approximate number of their records;

2) the given name, surname and contact details of the data protection officer or another contact person who can provide additional information;

3) the possible consequences of the personal data breach;

4) the measures taken by the controller to prevent the personal data breach and to minimise the possible adverse effects of the breach.

(4) If it is not possible to provide the information referred to in Paragraph three of this Section concurrently with the notification on the personal data breach, it shall be provided separately as soon as it is available.

(5) The notification of the personal data breach to the Data State Inspectorate may be omitted if this does not result in the risks to the rights and legitimate interests of the data subject.

(6) The controller shall document all personal data breaches by indicating related circumstances, consequences thereof and the measures taken for the prevention of breaches. The abovementioned information shall be provided by the controller to the Data State Inspectorate upon request.

(7) If a personal data breach requires the notification of the Data State Inspectorate and involves personal data that have been transferred by the controller of another Member State of the European Union or that have been transferred to the controller of another Member State of the European Union, the information referred to in Paragraph three of this Section shall be notified by the controller without undue delay to the relevant controller of the Member State of the European Union.

**Section 24. Notification of a Personal Data Breach to the Data Subject**

(1) If the personal data breach may result in a high risk to the rights and legitimate interests of the data subject, the controller shall, immediately after having become aware of the breach, notify the data subject thereof. The nature of the personal data breach shall be indicated and at least the information referred to in Section 23, Paragraph three, Clauses 2, 3 and 4 of this Law, and also the information on the measures taken for the prevention of the personal data breach, shall be included in the notification to the data subject.

(2) The notification of the personal data breach to the data subject shall not be required if any of the following conditions are met:

1) the controller has taken appropriate technical and organisational protection measures, in particular such measures that render the personal data unintelligible to any person who is not authorised to access the relevant data, and the abovementioned measures are applied to personal data affected by the personal data breach;

2) the controller has taken measures to prevent the high risk to the rights and legitimate interests of the data subject referred to in Paragraph one of this Section;

3) the informing of the data subject would involve a disproportionate effort. In such a case, public communication or a similar equally effective measure shall be used for informing the data subject.

(3) Irrespective of the conditions of Paragraph two of this Section, the Data State Inspectorate may request the controller to notify the data subject if the controller has failed to notify the data subject of the personal data breach.

(4) The notification of the personal data breach to the data subject may be suspended, restricted or omitted if the Law which governs the processing of the particular personal data provides for the processing of personal data without informing the data subject.

**Section 25. Designation of the Data Protection Officer**

(1) The controller shall designate the data protection officer. The same person may be the data protection officer of several controllers as well, if appropriate, and this person is able to effectively perform the tasks of the data protection officer.

(2) The controller shall notify the Data State Inspectorate of the designation of the data protection officer, and also publish the given name, surname and contact details of the data protection officer on its website.

**Section 26. Tasks of the Data Protection Officer**

(1) The controller shall involve the data protection officer in addressing all issues which relate to the protection of personal data, properly and in a timely manner, except for addressing such issues which arise within the scope of the administration of justice.

(2) The data protection officer shall have the following tasks:

1) to inform and advise the controller and its employees who perform the processing of personal data on their obligations in accordance with this Law and other laws and regulations regarding the protection of personal data;

2) to monitor the conformity of the internal regulations developed by the controller with this Law and other laws and regulations regarding the protection of personal data, including in respect of the assignment of responsibilities, awareness-raising and training of the persons involved in processing operations, and also to take other monitoring measures related to the protection of personal data;

3) to provide advice where requested as regards the assessment of the processing of personal data and monitor data processing;

4) to cooperate with the Data State Inspectorate;

5) to act as the contact person for the Data State Inspectorate in all matters related to the processing and protection of personal data;

6) other tasks assigned by the controller.

(3) The controller shall provide support to the data protection officer in the performance of the tasks assigned thereto by ensuring the necessary resources and access to personal data and processing operations, and also shall ensure the data protection officer the possibility to improve its knowledge in the field of the processing of personal data.

(4) The norms included in the Data Regulation and in the Personal Data Processing Law regarding data protection officers shall be applicable in respect of the competence, qualification, designation of the data protection officer and removal thereof from the list of data protection officers.

**Chapter V**

**Transfer of Personal Data to Third Countries or International Organisations**

**Section 27. General Principles for the Transfer of Personal Data**

(1) Personal data shall be transferred to a third country or an international organisation only if all of the following conditions are met:

1) transfer is necessary for the purposes referred to in Section 2 of this Law;

2) personal data are transferred to the controller in a third country or an international organisation which is competent to process personal data for the purposes referred to in Section 2 of this Law;

3) a Member State of the European Union or European Economic Area which has made personal data available or transferred them in accordance with its national law has given prior authorisation for transfer;

4) the European Commission has adopted the decision on the adequacy of the level of the protection of personal data in the relevant third country or international organisation, but if such decision has not been adopted, the requirements of Section 28 or 29 of this Law have been complied with.

(2) Personal data may be transferred to a third country or an international organisation without applying Paragraph one, Clause 3 of this Section if it is not possible to obtain the consent of the relevant country for the transfer of data, but the transfer of personal data is necessary to prevent an immediate and serious threat to public security of the country or essential threat to the interests of a Member State of the European Union. In such case, the authority of the country which is responsible for the giving of consent shall be informed immediately.

(3) Personal data shall be transferred further to another third country or international organisation if the competent authority which carried out the initial transfer or another competent authority of the same Member State of the European Union has given consent for further transfer after it has considered all relevant factors, including the severity of a criminal offence or an administrative offence, the purpose for which personal data were transferred initially, and the level of the protection of personal data in the third country or international organisation whereto personal data were transferred.

(4) Personal data shall be transferred in a way to ensure that the level of the protection of personal data is not undermined.

**Section 28. Transfer of Personal Data by Applying Appropriate Safeguards**

(1) If the European Commission has not adopted the decision on the adequacy of the level of the protection of personal data, the controller may transfer personal data to a third country or an international organisation if any of the following conditions are met:

1) appropriate safeguards for the protection of personal data are provided for in a legal act or contract binding upon the controller;

2) the controller has assessed all the circumstances surrounding the transfer of personal data and concluded that appropriate safeguards for the protection of personal data have been provided.

(2) If personal data are transferred on the basis of Paragraph one, Clause 2 of this Section, the controller shall have the following obligations:

1) to document the transfer of such personal data by indicating at least the personal data transferred, the justification for the transfer, the date and time of the transfer, and also the information on the competent authority which receives personal data. The relevant documentation shall be provided by the controller to the Data State Inspectorate upon request;

2) to inform the Data State Inspectorate on the categories of the personal data transferred.

(3) Insofar as it is not otherwise prescribed by law and international treaties and directly applicable laws and regulations of the European Union are not breached, competent authorities, without complying with that referred to in Paragraph one, Clause 2 of this Section, may transfer personal data to such recipients which perform commercial activities in third countries if all of the following conditions are met:

1) transfer of personal data is absolutely necessary for the performance of a task of the competent authority for the purposes referred to in Section 2 of this Law;

2) the rights of a data subject do not override the public interest for which the transfer of personal data is necessary in the respective case;

3) the transfer of personal data to the institution that is competent to process data for the purposes referred to in Section 2 of this Law is ineffective or inappropriate, in particular because the transfer cannot be achieved in due time;

4) the institution that is competent to perform data processing for the purposes referred to in Section 2 of this Law in the third country is informed without undue delay, unless it is ineffective or inappropriate;

5) the competent authority informs the recipient of the specified purpose or purposes for which the personal data may be processed by it if such data processing is necessary;

6) other requirements of this Law are complied with.

(4) In the case referred to in Paragraph three of this Section the competent authority which transfers personal data shall document the transfer thereof by indicating at least the personal data transferred, the justification for the transfer, the date and time of the transfer, information on the competent authority which receives personal data, and shall also inform the Data State Inspectorate on the transfer of personal data.

**Section 29. Transfer of Personal Data in Specific Situations**

(1) If the European Commission has not adopted the decision on the adequacy of the level of the protection of personal data or appropriate safeguards for the protection of personal data are not provided, personal data may be transferred to a third country or an international organisation if it is necessary for any of the following purposes:

1) to protect essential rights and legitimate interests of the data subject or another person;

2) to protect the rights and legitimate interests of the data subject if the transfer is provided for in an external law or regulation;

3) to prevent an immediate and serious threat to public security of a country;

4) in an individual case – for the purposes referred to in Section 2 of this Law or for bringing, enforcement or defending of legitimate claims in relation to the purposes referred to in Section 2 of this Law.

(2) Pursuant to Paragraph one, Clause 4 of this Section, personal data shall not be transferred to a third country or an international organisation if the rights of the respective data subject override the public interests.

(3) The controller has the obligation to document the transfer of personal data by indicating at least the personal data transferred, the justification for the transfer, the date and time of the transfer, and also information on the competent authority which receives personal data. The controller shall provide the documentation to the Data State Inspectorate upon request.

**Chapter VI**

**Supervisory Authority and Restrictions on Supervision**

**Section 30. Supervisory Authority**

The supervision of the processing of personal data and the application of this Law shall be performed by the Data State Inspectorate. The competence, tasks, and status of the Data State Inspectorate are laid down in the Personal Data Processing Law, unless it has been laid down otherwise in this Law.

**Section 31. Restrictions on Supervision**

The competence of the Data State Inspectorate does not include the supervision of the personal data processing operations related to the administration of justice and also the personal data processing operations which are carried out by the competent authority within the scope of operational activities.

**Chapter VII**

**Administrative Offences in the Field of the Processing of Personal Data and Competence within the Administrative Offence Proceedings**

**Section 32. Illegal Activities with Personal Data and Failure to Fulfil the Obligations of the Controller**

(1) For any illegal activities with personal data, a warning or a fine of up to two hundred units of fine shall be imposed on an official or an employee of a competent authority.

(2) For the failure to fulfil the obligations of the controller, including for the introduction of inappropriate (insufficient) technical and organisation requirements for data protection, for the failure to designate the data protection officer, a warning or a fine of up to two hundred units of fine shall be imposed on an official of a competent authority.

**Section 33. Competence within the Administrative Offence Proceedings**

Administrative offence proceedings regarding the violations referred to in Section 32 of this Law shall be conducted by the Data State Inspectorate.

**Transitional Provisions**

1. In exceptional cases which are related to a disproportionate effort the compliance of the automated systems which have been developed until 6 May 2016 with Section 19, Paragraph one of this Law may be ensured by the controller by 6 May 2023.

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

**Informative Reference to European Union Directive**

The Law contains legal norms arising from Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

The Law has been adopted by the *Saeima* on 8 July 2019.

President E. Levits

Rīga, 22 July 2019