



PHARE PROGRAMME TWINNING PROJECT NO. LV/2002/IB/OT-01
DATA STATE INSPECTION

Document 5

Activity 1.2

Preparation of recommendations and proposals for the improvement of the Latvian data protection legislation

Draft Amendment to the Personal Data Protection Law

written by

Dr. Thomas Giesen, Mārcis Gobiņš

August 2005



**Ludwig Boltzmann Institut für Menschenrechte
Mandated Body**



DATU VALSTS INSPEKCIJA

This publication has been produced with the assistance of the European Union. The contents of this publication can in no way be taken to reflect the views of the European Union.

The *Saeima* has adopted
and the President has proclaimed
the following law:

Amendment to the Personal Data Protection Law

The Law on the Protection of Personal Data (Latvijas Republikas Saeimas un Ministru Kabineta Ziņotājs, 2000, 9.nr.; 2002, 23. nr.) is amended as follows:

Section 3

(1) This Law applies, with exceptions set out in this Section, to processing of all types of personal data and to any natural and legal person if:

- 1) the system controller is registered in the Republic of Latvia; when the latter is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by this Law;
- 2) data are processed outside the borders of the Republic of Latvia, or in territories belonging to the Republic of Latvia in accordance with international treaties;
- 3) equipment which meant to be used for processing of personal data is located within the territory of the Republic of Latvia.

(2) In the cases referred to in paragraph 1, sub-paragraph 3 of this Section, the system controller shall appoint a person in charge of following the present Law.

(3) This Law shall not apply to information systems established by natural persons wherein personal data are processed for personal or household and family purposes and wherein the collected personal data are not disclosed to other persons.

- (4) This Law shall not apply in so far as a controller located in another member state of the European Union or in another state party to the Agreement on the European Economic Area processes personal data, except where such processing is carried out by an establishment in Latvia.

(...)

Section 11

The processing of sensitive personal data is prohibited, except in cases where:

- (1) the data subject has given his or her explicit written consent to the processing of his or her sensitive personal data;
- (2) special processing of personal data, without requesting the consent of the data subject, is provided for by regulatory enactments which regulate legal relations regarding employment, and such regulatory enactments guarantee the protection of personal data;
- (3) personal data processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express their consent;
- (4) personal data processing is necessary to achieve the lawful, non-commercial objectives of public organisations and their associations, if such data processing is only related to the members of these organisations or their associations and the personal data are not transferred to third parties;
- (5) personal data processing is necessary for the purposes of medical treatment, rendering health care services or administration thereof and distribution of medical remedies;
- (6) the processing concerns such personal data as necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings.

- (7) processing of personal data is necessary for rendering social aid and is performed by a provider of social aid services;
- (8) processing of personal data is necessary for establishment of the Latvia State Archives Fund is performed by state archives and institutions having the right of a state depository approved by the Director General of the State Archives;
- (9) processing of personal data is necessary for statistical research carried out by the Central Statistics Board;
- (10) processing relates to personal data published by the data subject him/herself.

Derogations from the first sentence of this section provided for in paragraphs 7,8 and 9 shall be notified to the European Commission.

Section 12

Personal data relating to criminal actions, previous conviction in criminal cases, court proceedings in criminal cases or closed court sessions on civil cases, shall only be allowed for processing by persons and in cases provided for by law. As far as the relevant law provides for derogations from the first sentence of section 11, these shall be notified to the European Commission. A complete register of criminal convictions may be kept only under the control of official authority.

(...)

Section 16

- (1) A data subject has the right to request that his or her personal data be supplemented or rectified, as well as that their processing be suspended or that the data be destroyed if the personal data are incomplete, outdated, false, unlawfully obtained or are no longer necessary for the purposes for which they

were collected. If the data subject is able to substantiate that the personal data included in the personal data processing system are incomplete, outdated, false, unlawfully obtained or no longer necessary for the purposes for which they were collected.

- (2) A data subject has the right to object at any time on compelling legitimate grounds relating to his particular situation to the processing of his personal data, save where there is no discretion with regard to the processing of personal data. Where there is a justified objection, the processing instigated by the controller may no longer involve those data.
- (3) The system controller must rectify any inaccuracies or violations of personal data protection provisions without delay, and furthermore notify any third parties who have previously received the inaccurate or incomplete data.

(...)

Section 21

- (1) Before carrying out any wholly or partly automatic personal data processing operation, public and private bodies shall notify such with the Data Supervisor, in accordance with the procedures prescribed in this law (notification).
- (2) The Data Supervisor examines the notification with regard to the observance of personal data protection provisions.
- (3) Personal data processing operations are exempt from the notification requirement if the data subject may obtain the data relating to him, and furthermore, either of the following applies:
 - 1) The controller processes personal data for his own purposes, provided that a maximum of twenty employees are concerned with the processing of personal data, and either consent has been obtained from the data subject, or the processing serves the purposes of a contract or a quasi-contractual fiduciary relationship with the data subject.

- 2) Processing operations refer to staff administration, bookkeeping or accounting only.
- 3) The sole purpose of the processing operations is the keeping of a register which according to laws or statutory orders, charters or bylaws is intended to provide information to the public and which is open to consultation either by the public in general or by any person demonstrating a legitimate interest.
- 4) The data are already published in accordance with the law, or they are taken from public registers.
- 5) Processing is carried out in the course of its legitimate activities and for purposes specified by bylaws by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body .
- 6) The controller has appointed a data protection official.

(4) The Cabinet of Ministers, upon consultation with the relevant professional organisations and in accordance with the Data Supervisor, is hereby authorised to exempt further groups of data processing operations from the notification requirement by regulation. When doing so, the Cabinet of Ministers shall take into account a combination of the following factors: the purposes of the processing, the data or categories of data undergoing processing, the category or categories of data subject, the recipients or categories of recipient to whom the data are to be disclosed and the length of time the data are to be stored.

Section 22

- (1) In so far as automatic personal data processing operations are subject to notification in accordance with Section 21, the following information shall be furnished:
- 1) the name and address of the data controller and of his representative,
 - 2) the purpose or purposes of the data processing,

- 3) a description of the category or categories of data subject and of the data or categories of data relating to them,
- 4) recipients or categories of recipient to whom the data can be disclosed,
- 5) standard periods for erasure of the data,
- 6) proposed transfer of data to third countries,
- 7) a general description which enables a provisional assessment to be made as to whether the measures under Section 25 to safeguard the security of processing are adequate and reasonable in relation to the necessary level of protection.

(2) Any changes or amendments of information referred to in paragraph 1 shall be notified to the Data Supervisor as soon as possible.

(3) The Data Supervisor shall decide whether a personal data processing operation is registered. Where this is the case, he issues a certificate of registration to the system controller. Otherwise, the data processing operation is prohibited.

(4) For each registration of personal data processing system or each registration of amendments mentioned in part four of this Section, a state fee is collected in accordance with the procedure and amount established by the Cabinet of Ministers.

Section 23

(1) Public and private bodies processing personal data may appoint in writing a data protection official.

(2) Only knowledgeable and reliable persons may be appointed as data protection officials. He shall not be exposed to any conflict of interests with regard to other duties by reason of his appointment. A person from outside a body concerned may also be entrusted with this duty.

- (3) The data protection official shall act independently in exercising the functions entrusted to him, and he shall have direct access to the head of the public or private body. He shall suffer no disadvantage for performing his duties in an assiduous manner.
- (4) Data subjects may approach the data protection official at any time. The data protection official shall be bound to maintain secrecy on the identity of the data subject and on circumstances permitting conclusions to be drawn about the data subject, unless he is released from this obligation by the data subject or by law.
- (5) Public and private bodies shall support the data protection official in the performance of his duties and, in particular, to the extent needed for such performance, make available assistants as well as premises, furnishings, equipment and other resources including education and training.
- (6) The data protection official shall work towards ensuring compliance with data protection provisions in sectoral or specific laws, or with this Act. In particular, he shall
 - 1) monitor the proper use of personal data processing operating systems; for this purpose the controller must in due time provide the data protection official comprehensive information about any projects for automatic processing of personal data;
 - 2) take suitable steps to familiarise the persons employed in the processing of personal data with data protection provisions in sectoral or specific laws, or with this Act.
- (7) The data protection official may inspect any files, databases or other data media, except personnel data, save with the consent of the data subject. He must be provided any information in relation to his duty on his request. He may also consult the Data Supervisor at any time.
- (8) Public and private bodies shall inform the Data Supervisor of the name of the data protection official and of the date of appointment within one month upon his appointment.

Section 23 a)

- (1) The controller shall provide the data protection official with an overview of the information stipulated in Paragraph one of Section 21a and a list of persons entitled to access the data processing system or systems. The data protection official shall, on request, make the information under Section 21a (1) Nos. 1 to 6 available to anyone in an appropriate manner.
- (2) In the event of Section 21 (5) the controller shall provide, on request, the information under Section 21 a (1) Nos. 1 to 6 to anyone in an appropriate manner.

Section 22 b)

- (1) In so far as automated processing operations involve special risks for the rights and freedoms of the data subject, they are subject to examination prior to the beginning of processing (prior checking). Prior checking shall be carried out in particular when
 - 1) sensitive personal data (Section 11) are to be processed or
 - 2) the processing of personal data is intended to appraise the data subject's personality , including his abilities, performance or conduct,unless a statutory obligation applies, the data subject's consent has been obtained or the processing serves the purposes of a contract or a quasi-contractual fiduciary relationship with the data subject.
- (2) The Cabinet of Ministers, upon consultation with the relevant professional organisations and in accordance with the Data Supervisor, may provide by regulation that further prior checking is carried out, in accordance with the conditions as spelled out in paragraph 1 of this article.
- (3) Prior checking has to be carried out by the data protection official who, in cases of doubt, shall consult the Data Supervisor. The results of the prior checking examination shall be submitted to the Data Supervisor. In case no data protection

official has been appointed the Data Supervisor shall carry out the prior checking following receipt of a notification of the controller.

(...)

Section 24

- (1) The State Data Inspection shall include the information mentioned in Section 22 of this Law (except for information mentioned in subparagraph 9 of paragraph 1 of the same Section) in the register of personal data processing systems. The register is a component part of national information system.
- (2) Information concerning the registered personal data processing systems shall be published in accordance with the procedures prescribed in regulatory enactments. Register mentioned in part one of this Section shall not include information on registered personal data processing systems, activity of which is governed by the Law on Official Secrets and the Law on Operative Activity.

(...)

Section 28

- (1) Personal data may be transferred to another state if that state ensures a level of data protection corresponding to the relevant level of the data protection effective in Latvia.
- (2) Exceptions from compliance with the requirements of paragraph one of this section are allowed if at least one of the following conditions is met:
 - 1) the data subject has given consent unambiguously to the transfer of the data to another state;
 - 2) the transfer of the data is required to fulfil an agreement between the data subject and the system controller, or the personal data are required to be transferred in accordance with contractual obligations concluded in the interest of

the data subject or also, considering request of the data subject, transfer of data is necessary for conclusion of a contract;

3) the transfer of the data is required and requested, pursuant to prescribed procedures, in accordance with significant state or public interests, or is required for judicial proceedings;

4) the transfer of the data is necessary to protect the vital interests of the data subject; or

5) the transfer of the data concerns such personal data as are public or have been accumulated in a publicly accessible register.

(3) Without prejudice to paragraph 1, a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of paragraph 2, where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights may be authorised by the Data Supervisor; such safeguards may in particular result from appropriate contractual clauses. The Data Supervisor shall inform the Commission and the other Member States of the authorizations he grants.

Section 29

(1) Supervision of personal data protection shall be carried out by the Data Supervisor. He promotes respect for the human right to inviolability of private life, home and correspondence and monitors the observation of these rights by all public bodies – including the President, the Saeima and the Courts, only insofar as they act administratively – as well as by all private parties. He acts in the interests of the bearers of this human right, and he supports the Saeima in its parliamentary control function in this area in a self-initiated way.

(2) The President of the Constitutional Court nominates and the Saeima, by a majority of no less than 51 votes, elects the Data Supervisor for a term of ten

years¹. He may not be re-elected. The Data Supervisor shall cease to hold his office subject to the same conditions as a Judge of the Constitutional Court.

(3) The Data Supervisor fulfils his duties pursuant only subject to the law, in complete independence in exercising the functions entrusted to him. He is subject only to the law. He is not part of the State “pārvalde” in the sense of Article 58 of the *Satversme*. Direct or indirect interference with the Data Supervisor in relation to his acting shall be prohibited. The Data Supervisor shall be under the disciplinary supervision of the speaker of the Saeima, insofar as his independence remains unaffected.

(4) Upon assuming his duties, the Data Supervisor shall take the following solemn oath or pledge at the Saeima:

“I, <NAME>, upon assuming the duties of the Data Supervisor, am aware of the responsibility that is entrusted to me and swear (solemnly pledge) to be fair and just in defending individuals’ right to inviolability of their private life, home and correspondence in compliance with the Constitution and the laws of the Republic of Latvia, as well as with the relevant international agreements that are binding on the Republic of Latvia.”

The Data Supervisor shall have a stamp, which shall comprise the picture of the small supplemented national coat of arms and the title of the Data Supervisor.

(5) The Data Supervisor is entitled to the same salary as the Auditor General, as well as to appropriate social and retirement guarantees. The Data Supervisor is entitled to his own budget position which is planned, defended and administered by himself. He is superior to his staff in all material and disciplinary matters. He may delegate his duties and the related rights to his staff.

¹ If a shorter term would be foreseen, then re-election should be possible. In any case, the Data Supervisor’s term should exceed the term of the Saeima.

Yet, it should be kept in mind that a short office term inevitably weakens the independence of the Data Supervisor. He would then be prompted to try to win the support of the governing majority for his re-election. This would be highly problematic in view of the fact that one of his main tasks is to control the Government.

Institutions, whose tasks it is to control the Government, should in principle not be put in a position to depend on the governing majority’s courtesy.

- (6) The official rights and duties of the Data Supervisor's staff, as well as their remuneration and social guarantees are the same as those of the staff of the State Audit Office.
- (7) The Data Supervisor has the right to remain silent about his official affairs in court or administrative procedures. In the same situation, the Data Supervisor or his staff cannot be compelled to disclose any data which they have acquired in the course of their official conduct.
- (8) The Data Supervisor and his staff must respect State secrets, human rights and business secrets, also upon termination of their work.
- (9) The Data Supervisor represents the Republic of Latvia in the relevant supranational and international bodies in the area of personal data protection. He offers administrative assistance to supervising authorities in the European Union member States, including the transmission of relevant data.

Section 30 a)

- (1) Every person, also every public official, may directly contact the Data Supervisor or his staff. This possibility must not be conditioned on giving any special reasons. Furthermore, a person must not suffer any disadvantages for contacting the Data Supervisor, except for knowingly providing false or misleading information.
- (2) The Data Supervisor advises and controls all administrative bodies, as well as all private parties in matters of personal data protection, with regard to all forms and all stages of a data processing operation. He acts on his own accord, or on the basis of complaints. He is entitled to address the President, the Saeima, its Committees and Sub-Committees and the Cabinet of Ministers.
- (3) The aforementioned, or a group of five Members of Parliament, are on their part entitled to require the Data Supervisor to investigate individual cases and to

report in due form on any aspect of his work, without detriment to his duty to observe human rights.

- (4) The Data Supervisor is entitled to freely enter any plots of land, State or private buildings or premises and inspect any files, databases or other data media during business hours. The Data Supervisor is not entitled to exert coercive power; for this, he may revert to police, prosecutor or courts. He may interrogate any private person or official, also confidentially. The private person's legal right to remain silent stays unaffected, as well as professional confidentiality rules. Every natural or legal person must answer the Data Supervisor's questions truthfully and without hesitation. Whenever a public official is called upon to disclose any type of information to the Data Supervisor, including official secrets, any confidentiality rules otherwise applying to him as a public official shall be disapplied.
- (5) The Data Supervisor registers personal data processing systems and cancels a certificate of personal data processing registration, if violations of law are established.
- (6) The Data Supervisor may summon the replacement of a data protection official if that person is not credible or incompetent.
- (7) The Data Supervisor may carry out checks of the compliance of personal data processing with the requirements of regulatory enactments. In cases where the law bars the system controller from informing the data subject of the processing, the data subject will be informed by the Data Supervisor only of the fact whether or not regulatory enactments have been observed in relation to him, as far as this does not jeopardise any lawful activities of the State or business secrets.
- (8) In collaboration with the Office of the Director General of the State Archives of the Republic of Latvia, the Data Supervisor decides on the transfer of personal data processing systems to the State Archives for the preservation thereof.

Section 30 b)

- (1) All institutions of the public administration must fully co-operate with the Data Supervisor, as the case may be, also under his auspices, and furnish him any information that he may require to fulfil his official duties. The Data Supervisor may contract external experts.

- (2) If the Data Supervisor finds that personal data processing regulations have been violated in a particular case by a public institution, he may
 - interrogate them and summon them to comment on the matter;
 - make recommendations and/or admonish them;
 - lodge a formal complaint with the heads of the public institutions concerned; this formal complaint should include an appraisal of the relevant facts, a reasoning and a conclusion with an identification of the data protection rules violated; it may also include a request to remedy the identified violations of personal data protection law and their effects; this request may include specific recommendations and/or orders to the public institutions concerned;
 - submit a copy of the formal complaint to the relevant minister who is in charge of the public institution concerned;
 - request the Cabinet of Ministers to comment on the matter;
 - submit the matter to the Saeima or any of its bodies for discussion and resolution, as the case may be;
 - inform the public about the matter;
 - bring an action in a court of law or with the Prosecutor's Office, in his own name or on behalf of others; court and administration fees are waived for the Data Supervisor.

The Data Supervisor is free in his choice and application of the above methods of intervention; he is bound only by the principle of proportionality.

- (3) The Data Supervisor is entitled to sit in and to speak at the Committees and other bodies of the Saeima, in accordance with parliamentary rules and

procedures. He is to be appropriately consulted by the Saeima or the Cabinet of Ministers when drawing up laws, administrative measures or regulations relating to the protection of individuals' rights and freedoms; the Data Supervisor may publish his views on those issues.

- (4) The Data Supervisor audits and accredits persons to perform personal data processing system audits in accordance with the law. The procedure of appointment and accreditation, as well as the procedure of withdrawal of an accreditation for grave violations of law are further regulated by the Cabinet of Ministers.
- (5) The Data Supervisor publishes an annual report on his activities; he may also publish any views that he may hold on relevant questions within his competence. The Data Supervisor may address and inform the public in any way, without detriment to his duty to respect the human rights of individuals – in particular, Article 6 of this law. Where the Data Supervisor does not address the public or act within his official capacity, he is bound by professional secrecy obligations.

Section 30 c)

- (1) The Data Supervisor may order private persons to process, block, erase or destroy data, impose a temporary or definitive ban on processing, or impose fines on private persons for violations of personal data protection rules according to the penal code.
- (2) The Data Supervisor may certify data processing systems or withdraw a certification; he may also certify individuals to issue seals of data protection compliance to other private persons or withdraw such certifications.
- (3) Administrative decisions by the Data Supervisor concerning private persons may be appealed against through the administrative courts by the person concerned.

The *Saeima* has adopted
and the President has proclaimed
the following law:

Amendment to the Constitutional Court Law

The Constitutional Court Law (*Vēstnesis* nr. 103, 14.6.1996) is amended as follows:

Section 17 (1)

9) The Data Supervisor.

(The previous sub-paragraph no. 9 becomes sub-paragraph no. 10; sub-paragraph 10 becomes 11; 11 becomes 12.)