



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

Document 24

Activity 4.3

Creation of material for an awareness campaign among data controllers and workshops / training for data controllers

Data Protection in the Public Sector

Brochure

written by

Lukas Gundermann

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.

1. Data protection - what is it all about?	2
2. What is in the Personal Data Protection Law (PDP Law)?	3
3. What is Personal Data?	3
4. Who is a system controller?	5
5. In which cases personal data may be processed lawfully ?	6
6. Which are the basic principles of data processing?	9
7. Are all personal data under the same level of protection or is there a distinction between more or less sensitive data?	12
8. Do you provide personal data to a data recipient?	13
9. Do you transfer personal data to foreign countries outside of the European Union?	13
10. What happens if my authority does not comply with the PDP law?	15
11. What does my authority actually has to do?	15
12. Does my authority has to appoint a data protection official?	19
13. How to deal with subject access request?	20
14. Does the State Data Inspection advise and help me?	22
15. Where I can get more information?	22

Introduction

The present paper is designed as a guide to work with the Latvian Personal Data Protection Law targeted particularly at public sector institutions: public authorities, municipalities, state run universities, public schools etc. It tries to answer data controllers' most frequently asked questions and should be understood as a valuable starting point in helping them to achieve compliance with the DPD Law.

1. Data protection - what is it all about?

While carrying out their responsibilities, public authorities have to collect a great amount of personal data of citizens. The data are stored, utilised it in certain ways, transferred to other parties and deleted at the end if they are not longer needed.

But personal information are not just data like any other. They are related to a human being, possibly reflecting some of his or her features, experiences or views on life. In a democratic society under the rule of law, persons' rights count most. One of these rights is their right to privacy and data protection as enshrined in the Latvian constitution, the European Convention on Human Rights and the Catalogue of Fundamental Rights of the EU. This includes the right to generally decide autonomously about the use of personal information. From this right the claim is derived to become informed about the use of one's personal data.

As a consequence, public authorities need a legal justification to deal with people's personal data. In most cases the legal ground can be found in a law, either a specific one or the general data protection law, the Personal Data Protection Law (DPD Law).

2. What is in the Personal Data Protection Law (PDP Law)?

The PDP Law aims to protect the individual's right to privacy, and to promote high standards in the handling of personal data. It seeks to strike a balance between the rights and freedoms of individuals, in particular the inviolability of private life, and the sometimes competing interests of those with legitimate reasons for using personal data.

The PDP Law applies to all processing of personal data by automatic means or by other means in structured filing systems (e.g. lists, card indexes, files, codes etc.). It places obligations on those who process information, the so called system controllers, while giving rights to those individuals who are the subject of that data.

Processing, in relation to data, means collecting, recording or holding the data or carrying out any operation or set of operations on the data, including e.g. accumulation, classification, grouping, combinations, alteration, providing, making available, use, logical and/or arithmetic operations, retrieval, dissemination, destruction, etc. (cf. Sec. 2 No. 4)

Some general legal grounds for lawful data processing are laid down in Section 7 of the DPD Law; other laws might contain specific regulations. In addition, the fair processing principles have to be observed. In Section 10 DPD Law it is stated inter alia that personal data must be used for specified purposes and only to the extent required for that particular purpose.

3. What is Personal Data?

The scope of data protection is "personal data" of an individual. Personal data is any information related to an identified or identifiable natural person. The term "information" includes also sounds and images (e.g. photos, video). It might refer to any aspect of the persons' lives, whether their business lives, professional lives or private lives. The concept of data "relating" to an individual is very wide. Personal data are not limited to private or family data nor is there any particular way in which the data must relate to an individual. It might be in any aspects of their lives, whether their business lives, professional lives or private lives. This addresses all kind of information relating to a person, including both, facts and opinions.

To signify the person concerned by this information, the data protections laws use the term "data subject". Personal data can be linked to a data subject either directly or indirectly. It is linked directly if identifying information is available together with the respective data.

<p>Example: A data base contains information of recipients of social welfare (as amount of funding, date of payment), including identifying information as names and addresses. For everybody who has access to this data base, all information on social welfare funds are personal information about the recipients, the "data subjects".</p>

Information relates indirectly to a data subject in cases where the assessment of the existing information allows concluding the identity of a person. This sort of personal data may be found e.g. in statistical information.

Example: The only foreigner living in a small village; the person paying a high amount of taxes and running a certain business.

Indirect reference to a person may also be effected by referring to a specific identifier which contains no direct addressing information in the first place but can be linked to such information. In these cases the data in question is personal data if the organisation storing and using the data has lawful means to access the additional identifying data.

Example: From the number of a car licence plate, most people won't be able to tell the name of the holder. In contrast to them, the authority responsible for registering cars in principle holds the technical and legal possibility to find out the holder of the car. The same is true for authorities to whom the respective information is allowed to be disclosed in a lawful manner.

Example: The personal identity (classification) numbers used in Latvia can be linked to personal information whenever the entity storing it also holds the primary identifying addressing data of a person as his name or has the legal possibility to access the respective data base. Consequently, a personal identity (classification) number is to be regarded as personal data in most circumstances.

Example: Under certain circumstances also an IP address, which is a unique number used by computers to address each other when sending information through the Internet, can be personally identifying information of the user. This is the case where an access provider stores identifying addresses of subscribers together with the IP numbers assigned to the respective users for a certain time period.

The legal protection by the DPD Law is limited to natural persons as data subjects; legal persons are excluded from the scope of protection. However, information about a legal person can be at the same time related to a natural person.

The term "natural person" means a living individual. The post mortal rights of a person may be protected by other laws; however they do not fall within the scope of the data protection law.

Example: The information on the cause of death is not protected by the data protection legislation. However it may fall within the scope of different laws obliging at least members of certain professions to keep the information confident (see e.g. for doctors Art. 50 of the Medical Treatment Law).

4. Who is a system controller?

Most public authorities have to deal with citizens' personal data in order to fulfil the responsibilities put upon them. According to the DPD Law, a natural or a legal person who determines the purposes of a personal data processing system and means of processing is defined as system controller in the sense of the law. In other words, a system controller is the party who decides on the collection of personal data and the purposes they are used for. Most reasons respectively purposes of processing in the public sector are predefined by law. But these laws do need to be executed. This is done by the authorities implementing the laws. By way of implementing them, the authorities also decide on technical means like the establishment of data processing systems. Thus, most public authorities and other public sector bodies are system controllers according to the DPD Law.

Example: A law on population register may constitute the obligation to install such register; the implementation is assigned to a certain authority. Consequently, the latter authority is the system controller in the sense of the DPD Law.

Sometimes it turns out to be necessary to assign certain tasks with view to personal data processing to a third person, a company or another public body. Such contractor does not necessarily have to be a system controller himself in the sense of the law. In many cases the contractor acts only on instructions given by the system controller and has no legal power to determine neither the purpose of the processing nor the particular processing actions (such as transferring data to a third body, using them in special way to create new information etc.). In these cases the contractor is to be regarded as operator of personal data as defined by the DPD Law. The characteristic of the operator is the fact that he is authorised by a system controller to carry out personal data processing upon the instructions of the system controller.

Example: A public authority decides to set up e-government services via WWW. It engages a company specialised in web portals to implement the service. The company is only supposed to provide its expert IT knowledge in order to realise a solution according to the concept of the public authority. After establishing the system, it is maintained by the private company. The company is only allowed to modify the system on request of the authority. In this case, the public authority remains system controller, the private company is an operator of personal data.

The system controller retains full responsibility for the actions of the operator. The DPD Law also introduces specific obligations upon data controllers when the processing of personal data is carried out on their behalf by operators of personal data; in particular a contract has to be signed (cf. Section 14 of the DPD Law).

5. In which cases personal data may be processed lawfully?

The Latvian DPD Law contains certain criteria for the lawful processing of personal data. In addition, some sector specific laws may contain special regulations for particular fields of administration. The latter are applicable to the respective authorities active in the field.

Example: The penal procedure code sets forth the rights to process personal data for the purpose of criminal prosecution procedures.

Where such laws do not apply, the general rules enclosed in the DPD Law have to be complied with. Personal data processing is permitted only if at least one of the conditions stated below exist. For public sector authorities, mainly the following of the lawful processing criteria are relevant:

- The data processing is necessary in order to exercise functions of an official authority vested in the controller.

This variant is the most relevant one for the public sector.

Personal data processing may be performed under the precondition that a certain responsibility is assigned by formal legal act to the respective authority. Yet, the extent is limited to the processing operations necessary for the exercise of the authority. To test the lawfulness of the extent of data processed and processing operations performed, it should be attempted to find a reasonable argument why processing operation and data are of particular necessity.

Example: In order to decide on applications for social welfare grants it will be necessary to assess the state of indigence of the applicant. Depending on the criteria which are relevant according to the law, the respective data may be collected, e.g. whether the applicant holds a bank account. In the first place, the applicants may be requested to provide respective information; if doubts regarding the credibility should arise, other ways of evaluating the situation (i.e. collecting data) may be chosen if they were provided by law.

The collecting of personal data can also be effected by receiving data from a third party as long as it is necessary for exercising the official authority. This gives state institutions the right to lawfully receive data from both, other public and private sector bodies. But this right to receive data does not imply the obligation of private sector institutions to disclose the respective data to the potential recipient; only where a special legal obligation is laid down by law, such an obligation might arise (as e.g. in proceedings in

criminal matters under certain prerequisites). Moreover, there may even be situations where the private sector controllers are prevented from disclosing data to public bodies under specific rules such as professional secrets for certain professions or contractual obligations in certain areas as the bank sector.

Example: In the above case, from the permission of the social welfare authority to collect data it can not be derived an obligation of the private bank to disclose the respective data of its clients. Unless such obligations are set forth in sector specific laws, the bank is not obliged to answer the request.

Example: The police is requesting certain information on a client from a bank in a criminal procedure. According to the Criminal Procedure Act the bank may be obliged to disclose the information.

Different rules apply to the public sector controllers: According to the principals of administrative assistance they are obliged to disclose data if the public sector recipient has the legal permission to collect it.

Example: In order to decide on the social welfare application mentioned above, the authority responsible needs to know an additional detail from another public body. The latter is obliged to provide the information in most cases, if the recipient is permitted to collect it.

- The data processing is necessary to protect vitally important interests of the data subject, including life and health.

In exceptional cases, this criterion may be applied by public sector system controllers.

- The data subject has given his or her consent.

Consent is only legally effective if it is a freely given indication of one's will. With view to public sector processing of personal data, the voluntariness of the consent is of crucial importance. Most relevant processing operations in the public sector are defined by law; the respective regulations set forth the categories of data which are permitted to be processed. In such cases, it is not admissible for public authorities to collect additional data on the basis of an alleged consent. Firstly, citizens dealing with public authorities in most situations do not have a real choice to decide on whether to disclose their personal information. Thus, a declaration of consent in these situations does not meet the requirements of a legally valid consent.

In addition, adding new categories of data on a presumed voluntary basis to the ones which are defined by law amounts to the extension of the authorities' competences -

done in an unconstitutional way without involving the parliament for whom it is to decide on the competencies of public authorities.

Consequently, the consent of the data subject may only serve as legal basis for personal data processing in exceptional cases where people have real freedom of choice.

Example: The local authority responsible for granting the Guaranteed Minimum Income, according to the Sociālo pakalpojumu un sociālās palīdzības likums [Social Services and Social Assistance Act], has to collect data on existing securities of the applicants, further on debt commitments, property which may be used to gain income etc. Yet, the granting of the benefit is not based on the person belonging to a certain group of society (for example, single mothers or pensioners, or people with disabilities). Therefore it would not be admissible for the respective authority to collect additional data from the applicants on an alleged voluntarily basis, such as being member of a specific group of society or belonging to some ethnic group, even if the applicants signed a declaration agreeing to such data collection.

Example: In order to be prepared for unexpected emergency situations it can be useful for a public authority to hold a list of members of special professions, such as physicians or engineers also including data which is not publicly available, as private addresses etc. If there is no specific regulation allowing such collections of data, it could be based on the consent of the data subjects, if they can freely choose whether to be included in the list or not.

Consent of the data subject is defined by the DPD Law as “a freely, unmistakably expressed affirmation of the wishes of a data subject, by which the data subject allows his or her personal data to be processed according to information delivered by a system controller”. The fact that the data subject must “unmistakably express” his affirmation means that there must be some active communication between the parties. System controllers cannot infer consent from non-response to a communication. A data subject may “express” affirmation other than in writing. On the Internet an electronically consent can be sufficient.

The consent has to be specific and informed, i.e. the data subject must be aware of the fundamental nature and the conditions of the processing and any important features which might particularly affect him, such as possible data recipients. As a result, vague and generalized consent declarations are inadequate.

Example: In the example given above (contact addresses of physicians etc.), it should be detailed the purpose of the data stored (use in particular situations...), possible recipients (other public authorities with special responsibilities in certain situation, as police, fire department...) duration of storage (e.g. 2 years, update after that time period).

Finally it must be recognized that even when consent has been given it will not necessarily endure forever. While in most cases consent will endure for as long as the processing to which it relates continues, you should recognize that, depending upon the nature of the consent given and the circumstances of the processing, the individual is entitled to withdraw consent at any time.

6. Which are the basic principles of data processing?

As a system controller a public authority has to comply with the four general principles of data processing set out in the PDP Law (Sec. 10). :

- Personal data must be processed fairly and lawfully.

To comply with this fundamental principle, personal data shall not be processed unless at least one of the criteria for lawful processing set out in the PDP Law is met (see question 5 above). The principle also requires system controllers to inform the data subject about the purposes for which the data are intended to be processed (see question 11 below).

Example: Data processing is unfair and unlawful, if personal data is collected secretly without notifying the data subject unless sector specific laws permit to do so (e.g. in the way of law enforcement).

- Personal data must be collected for specified purposes determined before collecting and later processed in accordance with the intended purpose and only to the extent required therefore.

As pointed out above, for public authorities in most cases the purposes of data processing are predefined by law. Still the public authorities have to implement the laws. This includes in most cases to decide about the commencement of personal data processing as well as the details of the system. When doing so, the public sector system controllers are restricted in transferring the data to other bodies for purposes different than the ones defined by law.

Example: A farmer has to indicate personal data to apply for agricultural subsidies. These data may not be transferred to other bodies outside the public sector, e.g. to manufacturers and resellers of certain agricultural products as basis to contact potential costumers.

The system controller is also precluded from using the data himself in a way and to a purpose different than prescribed by law.

Example: In the above case, the public authority collecting the data in order to decide on the applications may not create a data base serving purposes others than management of the subsidy applications. Insofar it is restricted to the purposes predefined by law.

However, it has to be borne in mind that the data processing is allowed in order to fulfil the functions of public authority vested by law. From this the consequence arises that the data transfers and usages are lawful in cases where the system controller and/or the data recipient collect and process the data in order to execute a specific responsibility assigned to them by law.

Example: In the above case, while assessing the applications for agricultural subsidies, it becomes apparent that the farmer has infringed upon certain ecological standards. If a public authority is furnished with the responsibility to enforce the respective standards and to impose fines on perpetrators, it is also allowed to process the personal data necessary to conclude this task. Therefore, the farmer's data may be transferred to the latter authority by the first one which is responsible for deciding on the application for subsidies.

The purpose of data collection should be indicated in some document, even though it might be perfectly clear for the authority collecting data. In particular, there are two means by which a system controller can specify the purpose for which personal data are obtained: the first is a notice given by the system controller to the data subject; the second is the notification which has to be effected to the supervisory authority (Data State Inspection) under the notification provisions of the PDP Law* (see question 11 below).

In complying with this principle, system controllers should also seek to define the minimum amount of data necessary in order to properly fulfil the tasks assigned to them. If it should turn out to be necessary to hold additional information about certain individuals, such information should only be collected and recorded in cases where the particular necessity arises.

Example: To decide on the applications for farm subsidies a certain set of data will be necessary. These data may be explicitly defined by law. In other cases, the authority has to define the minimum set of information which can not be omitted to decide on the application.

- Stored in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected and processed.

To comply with this principle, system controllers will need to review their personal data regularly and to delete or anonymise the information which is no longer required for the intended purposes. As it is not convenient to analyse each single set of data, there should be standard storage periods applied to each particular procedure personal data is used in.

In the public sector, terms for storage of personal data are scarcely defined by laws, even if the set of data to be stored is set forth in a legal regulation. In these cases, the system controller has to define a standard storage period himself. The definition of the term should start from a general evaluation of the period personal data is needed on an average for fulfilling the respective task plus some extra time as precaution for unforeseen circumstances.

Example: Personal data is being processed in a procedure where farmers apply for agricultural subsidies. Given the case that the funds are granted on a yearly basis and that the fact of granting the fund is relevant for the follow up application in the next year. In such a situation, data had to be stored at least for one year after the year of the grant. In practice, an additional term of one year might be added, so that the data had to be deleted at the end of the second year after the year in which the fund was granted, unless the data subject has filed a new application. The respective authority has to draw up internal rules, defining this term.

Moreover, it has to be borne in mind that there might be the obligation according to archive laws to deliver parts of the files and data bases which are no longer necessary to some state or local archive. Usually, it is up to the archive to decide on which material is regarded as worthwhile storing in the archive for a longer term. In delivering the material to the archive, the system controller also passes over responsibility for personal data included in the material; consequently, from his point of view the delivery to an archive equals the deletion of the material. Access to the archive and other details on how the material is to be treated is set forth in the archive laws.

- Accurate, and, when necessary for the processing of personal data, kept up to date.

Data are inaccurate if they are incorrect or misleading as to any matter of fact. Inaccurate or incomplete data must be rectified, supplemented, erased in a timely manner or their further processing must be restricted. In the public sector, this has to be done ex officio.

Example: While doing some routine check on the data base a public authority notices a mistake in one set of data: the data subjects' birth date is obviously incorrect. The system controller has to correct it by himself, without waiting for a respective request of the data subject who in most cases will not know about it. If the correct data cannot be found out from other data bases or files, the data subject has to be asked to indicate the correct date.

Example: When working with files containing personal data, it becomes apparent that a relevant change has not being included: A person changed name after marriage which is not reflected in the files. In this case the information in the files became incorrect because of subsequent changes of the facts of life. In such cases the information in the files should be updated, indicating that an update took place, reflecting the real life event. So the entry in the file could be amended by an annotation, stating the change of name and the underlying event. This way, the file is corrected but still contains the original information which was not incorrect at the time it was entered.

7. Are all personal data under the same level of protection or is there a distinction between more or less sensitive data?

Under the PDP law, specific provision is made for processing sensitive data. This includes racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, physical or mental health condition, sex life, criminal proceedings or convictions (cf. Sec. 2 No. 8).

This list derives from the EU Directive being the blueprint for the Latvian data protection law. The idea behind this list of specific data is that they might be of special harm to the data subject when used in certain ways.

Example: The fact, that somebody is member of a trade union could affects him negatively in certain situations, for instance in connection with the application for employment. This is why the trade union is required to keep your data in confidence.

For such data to be considered lawfully processed, at least one of the following conditions must be met:

- the data subject has given his or her explicit written consent;
- processing is necessary for the purposes of carrying out the obligations and specific rights of the system controller in the field of employment law in cases provided by regulatory enactments;

- processing is necessary to protect vital interests of the data subject or of any other person, where the data subject is unable to give his consent due to a physical disability or because he is legally incapable;
- processing is necessary to achieve the lawful, non-commercial objectives of public organizations and their associations on condition that the processed data relate solely to the members of these organizations or their associations and the personal data are not disclosed to third parties without the consent of the data subjects;
- personal data processing is necessary for the purposes of medical treatment, rendering health care services or administration thereof and distribution of medical remedies;
- the processing concerns such personal data as necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings;
- the data have been manifestly made public by the data subject.

For public authorities, additional regulations might be found in sector specific laws.

8. Do you provide personal data to a data recipient?

If so, this is only lawful on the basis of either a written request or a contract, if not prescribed otherwise by law (Sec. 13 Par. 2). The contract must specify the purposes for which the data will be used, the conditions and the procedure of its use. The request must specify the intended use of the data.

It is important to bear in mind that both, the request and the contract, are an additional prerequisite for lawful processing. Each transfer of personal data must be based on a legal ground as mentioned above in question 5.

Example: If it is permitted for state registers (e.g. population register) to disclose personal data to certain recipients, a contract has to be signed if this is a regular data transfer. In the case of a one-time transfer a written request will be sufficient.

Please notice that in the public sector, a lot of regular transfers is defined by law. These regulations may exempt the system controller from the obligation mentioned above.

9. Do you transfer personal data to foreign countries outside of the European Union?

In certain cases, public authorities might be requested to transfer data to foreign countries. If EU Member States are concerned, the transfer is permitted according to the same rules which are applicable to inner Latvian transfers. This is because the EU Directive on data protection obliges all Member States to create rules similar to the ones in force in Latvia.

Transfers of personal data to foreign countries which are no member states of the European Union (so called third countries) is subject to particular regulations. In principle, an authorisation issued by the State Data Inspection (SDI) should be applied for. If there is an adequate level of data protection in those countries the SDI has no discretion to withhold authorization. An authorization to transfer personal data to a third country without a generally adequate level of protection may be granted (the SDI has discretion insofar) by the SDI if adequacy is ensured by contractual or self-regulatory means.

Example: Such a contract may also be an administrative agreement between two public agencies (e.g. a Latvian police authority and a police authority in a third country) when the transfer of personal data in police matters is in question. Since it is vital that data which are to be transferred for specific purposes should be limited to these purposes in the importing third country the agreement should be made between two authorities which can make such agreements binding for all relevant public institutions in the importing country (normally a Ministry).

An authorization by the SDI is not necessary only if

- The data subject has given his unambiguously consent to the data export.

Example: If you wish to transfer a database containing records about many individuals to a third country, then – in order to rely on this provision – you need to obtain the consent of each one of these individuals before you can transfer their data.

- 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;
- 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;

Example: The exchange of data between tax and customs administrations or social security agencies.

- the data transfer is necessary in order to protect the vital interests of the data subject or

Example: Before relying on this provision, system controllers must first establish whether it is possible to obtain the data subject's consent. Only if this is not possible – for example due to urgency of time – can this provision be invoked.

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

Example: If a public authority, based on sector specific laws, runs a register which is publicly accessible, e.g. via internet, also access from third countries is justified by this provision.

10. What happens if my authority does not comply with the PDP law?

In a democratic state under the rule of law it is a basic principle for public authorities to comply with all legal regulations applying.

In cases of non-compliance, the Data State Inspection (DSI) could take enforcement actions against your authority to bring your processing into compliance with the principles.

Notice that the illegal processing of personal data, the violation of the data subjects rights and the non-fulfilment of lawful DSI orders can result in a fine.

An individual may also seek compensation through the courts for any damage suffered (Sec. 31).

11. What does my authority actually has to do?

- Informing the Data Subject

The precondition of legitimate processing of an individual's data is that he or she is informed about the fact that data processing is being carried out (Sec. 8). When data are obtained directly from data subjects you must ensure that the data subjects have, are provided with, or have made readily available to them, the following information:

- your identity and your permanent place of residence,
- if you have authorized an operator of personal data, the identity of that operator,
- the purpose or purposes for which the data are intended to be processed, and
- at the request of the data subject any further information which is necessary, taking into account the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair:
 - data recipients and purposes of the disclosure,
 - existence of the subject's right of access and rectification,

- consequences of a data subject's refusal to submit data to the system controller.

Example: In a certain administrative procedure, it is required by law that a different public authority is involved to give its opinion on the data subject's application. The data subject should be informed about the fact that his personal data is going to be disclosed to that third party. If the application is filed by submitting a written application form, on this form the information of the data subject could be included.

Note that the information is not demanded where the data subject already knows about the processing of his personal data.

As the PDP Law makes no specific provision relating to timescale in the case of data obtained from a data subject, the fair processing information must be provided to the data subject at the time that the data are obtained.

The fair processing information should also be provided to data subjects in cases where the data have been obtained from someone other than the data subject. Should the data not have been actively collected, the information has to be given at the time when the data are to be disclosed for the first time to third persons. In addition to the information mentioned above the data subject has to be informed about the categories and sources of the personal data which are being collected or will be collected (Sec. 9).

Example: A public authority receives a file from another authority handing over the case to the recipient who turned out to be the body actually responsible. If the file contains personal data, the data subject has to be informed by the recipient of the fact that it started to process the subject's personal data. If the authority who held the file first had already informed the data subject, the information by the data recipient is dispensable.

The fair processing information is not applicable in cases provided in the law. Such regulations might be found in sector specific laws as for example on criminal investigation procedures.

Moreover, the obligation to inform the data subject in cases of collecting data from others sources than the data subject itself does not apply to the processing of personal data for scientific, historical or statistical research, or establishment of state archives fund if the informing of the data subject requires inordinate effort or is impossible.

- Notifying on data processing by automated means

A further obligation of system controllers is to notify the State Data Inspection (SDI) about certain details of the processing operations, including the types of data they hold and the purposes for which they process personal data. The SDI examines this

notification with regard to the observance of personal data protection provisions and decides whether a personal data processing operation is registered. Where this is the case, it issues a certificate of registration to the system controller. Otherwise, the data processing operation is prohibited.

The principal purpose of having notification and a public register of system controllers – maintained by the SDI – is transparency or openness. The public should know or should be able to find out who is carrying out which sort of processing of personal data.

Please notice that – pursuant to Sec. 21 of the PDP Law* – notification is only required in the case of data processing by automated means, i.e. operations performed upon personal data carried out in whole or in part by automatic means.

Under Sec. 22 of the PDP Law* information to be provided to the SDI include

- the name and address of the data controller and of his representative, if any;
- the purposes or purposes of the data processing;
- a description of the category or categories of data subject and of the data or categories of data relating to them;
- recipients or categories of recipient to whom the data can be disclosed;
- standard periods for erasure of the data;
- proposed transfer of data to third countries;
- 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.

Exceptions of the notification regime are provided in the Law (Sec. 21 Par. 3*) for cases, when the data subject may obtain the data relating to him, and furthermore, one of the following applies:

- 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.
- Processing operations refer to staff administration, bookkeeping or accounting only.
- 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.
- The data are already published in accordance with the law, or they are taken from public registers.
- 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 .
- The controller has appointed a data protection official (see question 12 below).

- Notifying on prior checking

Particular categories of processing are subject to prior checking (Sec. 22b*). The requirement of prior checking means that the planned data processing operations may only take place if they have been examined prior to the start. Such prior checks shall be carried out by the data protection official (see question 11 below). The results of the prior checking examination have to be submitted to the SDI. If no data protection official has been appointed, the SDI itself is obliged to carry out the prior checking. In all these cases the system controller has to notify the SDI before the commencement of the intended data processing.

Prior checking is prescribed in cases of processing of sensitive data (Sec. 11) and when the processing of personal data is intended to appraise the data subject's personality, including his abilities, performance or conduct. Exceptions are provided in the PDP Law (Sec. 22b Par. 1*) in cases where

- 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.

- Implementing Data Security Measures

The security of personal information is all-important. It will be more significant in some situations than in others, depending on such matters as confidentiality and sensitivity. High standards of security are, nevertheless, essential for all personal information.

The Law (Sec. 25) requires the system controller and a possible operator of personal data to implement appropriate organisational and technical measures, which would ensure the protection of personal data against any accidental or unlawful destruction, alteration, and disclosure and against any other unlawful processing. These measures must ensure a level of security appropriate to the nature of the data to be protected and the risks represented by the processing. They cover e.g. access control, encryption, anti-virus software, firewalls, logs and audit trails, back-up systems, etc.

The mandatory technical and organizational requirements for the protection of personal data processing systems are defined in the Republic of Latvia Cabinet of Ministers Regulations No. 40 (available at <http://www.dvi.gov.lv/eng/legislation/requirements/>).

If you authorise a personal data operator to process personal data, you must choose an operator providing guarantees in respect of adequate technical and organisational data protection measures and ensuring compliance with those measures. Further on you shall stipulate that personal data must be processed only on your instructions. The relations between you and the personal data operator shall be regulated by a written contract (Sec. 14).

The employees of the system controller, the data processor and their representatives who are processing personal data must keep confidentiality of personal data if these personal data are not intended for public disclosure. This obligation shall continue after

leaving the public service, transfer to another position or upon termination of employment or contractual relations (cf. Sec. 27).

12. Does my authority have to appoint a data protection official?

The establishment of data protection officers by public and private sector organisations is a current international development. Even in the USA – where no general data protection law is in force - more and more companies appoint a “Data Privacy Officer” voluntarily. The EC Data Protection Directive 95/46, which is the basis for the Latvian DPD Law, allows the establishment of data protection officers in the national law of the EU member states as an option. In the meantime more and more member states make use of this opportunity (France, Germany, Latvia, Luxembourg, Slovakia, The Netherlands).

According to Sec. 23 (1)* public and private bodies processing personal data may appoint in writing a data protection official (DPO). Thus, appointing of a DPO is just an option for the system controller, but no obligation. Relating to the function a DPO is a kind of outsourced State Authority, that means that a DPO performs the same obligations which otherwise would have to be performed by the supervisory authority. For this reason, the DPO may consult the supervisory authority at any time (Sec. 23 (7)*), e.g. in case of doubt or of conflicts with the system controller. A considerable advantage of appointing a DPO is that the system controller does no longer have to notify its data processing activities to the supervisory authority (Sec. 21 (3, lit. 6)*).

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 system controller. He shall suffer no disadvantage for performing his duties in an assiduous manner (Sec. 23 (3)*). Therefore the DPO is free of any instructions concerning the fulfilment of his or her function. The DPO shall report directly to the director or head of the public authority.

The data protection official shall work towards ensuring compliance with data protection laws. In particular, he shall

- monitor the proper use of personal data processing operating systems (Sec. 23 (6, lit.1)*);
- inspect any files, databases or other data media, except personnel data, save with the consent of the data subject (Sec. 23 (7)*);
- take suitable steps to familiarise the persons employed in the processing of personal data with data protection law (Sec. 23 (6, lit. 2)*).

Therefore the DPO has to check and supervise legal compliance of the data processing activities of the system controller and to carry out specific training of employees on data protection issues. Training of employees and promotion of awareness can also be made by sending appropriate emails to the relevant staff members.

Only knowledgeable and reliable persons may be appointed as DPOs (Sec. 23 (2)*). That means that the DPO has an adequate education or relevant professional experience. Furthermore the DPO should be able to proof which training activities were carried out in the past to remain knowledgeable. Severe wrong decisions in data protection matters can cause a deprivation of the assumption of sufficient knowledge of

a DPO. As far as a DPO makes himself or herself liable to prosecution the necessary reliability for performing this function may disappear. Also violation of confidentiality (Sec. 23 (4)*) might damage reliability.

The DPO shall not be exposed to any conflict of interests with regard to other duties by reason of his or her appointment (Sec. 23 (2)*). Therefore the director or deputy of a public authority as well as the person responsible for staff management should not be appointed as DPO. The same is true for the persons responsible for IT within the public authority, since there might arise a conflict in this field.

A person from outside of the public authority may also be appointed as DPO (Sec. 23 (2)*). An external DPO generally has the necessary special knowledge to consult the system controller in a proper way so that the education of an internal employee is not necessary in this case. External DPOs can give valuable advice to handle data protection issues in a striking and cost-effective way.

Data subjects may approach the data protection official at any time. On their request confidentiality has to be guaranteed, preventing the DPO from revealing the identity of the complainant to the system controller (Sec. 23 (4)*). Therefore the DPO is the appropriate person to turn to, as far as a data subject is concerned about a violation of privacy. The DPO is responsible to support clearing up of any data protection issues.

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, office facilities, equipment and other resources including education and training (Sec. 23 (5)*). The DPO must be provided with any information in relation to his duty on his request (Sec. 23 (7)*). The system controller has to cooperate together with the DPO, to include the DPO in appropriate projects, and to grant access of the DPO to relevant information. Adequate equipment for performing the duties of a DPO might be a PC or laptop, access to the Internet, access to e mail, availability of telephone or mobile phone, availability of encryption software, and a work environment which guarantees confidentiality. The DPO should regularly participate in trainings and education measures to maintain special knowledge state of the art.

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 (Sec. 23 (8)*). Appropriate forms will be available at the Data Supervisor or on the Data Supervisor's webpage at <http://www.dvi.gov.lv/>.

13. How to deal with subject access request?

The PDP Law gives individuals certain rights regarding information held about them (Sec. 15). The key right for the data subject is the right of access. Essentially this means, that you, as a system controller, have to inform the data subject on his enquiry, whether you or someone else on your behalf hold personal data about that data subject and if so, to give a description of what these data are, the purposes for which they are being processed and those to whom they are or may be provided.

Example: A proper information could look as follows: “We are storing the following information on your person for the purpose of handling your application: name: John Q. Citizen; details collected by filling in the application form: family status, income ...”

As the case may be you have to inform as well about the date when the personal data concerning the data subject were last rectified, deleted or blocked, the source from which the personal data were obtained – unless the disclosure of such information is prohibited by law – and the processing methods utilized for the automated processing systems, concerning the application of which individual automated decisions are taken.

The individual is also entitled to have communicated to him in an intelligible form, all the information which forms any such personal data. Consequently, the data subject should be given a further explanation, where the system controller holds the information in coded form which cannot be understood without the key to the code.

Example: It is not sufficient to just provide the data subject with a coded list of data printed from a data base, e.g. John Q. Citizen, table field 2 - score 2, table field 3 - score 23, and so on. An intelligible form requires that the meaning of the code numbers is explained, e.g. score 2 in field 2 stands for unmarried, score 23 in field 3 stands for mentally challenged and so on.

System controllers must comply with a subject’s access request promptly, in other words as quickly as they can, and in any event within one month of receipt of the request. On enquiry information must be provided to the data subject in written form.

In order to ensure compliance with the time limit and other access obligations the following organisational and procedural steps are recommended:

- Appoint a coordinator who will be responsible for the response to access requests. All subject’s access matters should be submitted to the coordinator.
- Check the validity of the access request.
- Check that sufficient material has been supplied to definitively identify the individual. This is most important. You should set down criteria on what is sufficient to prove identity for your organisation.
- Check that sufficient information to locate the data has been supplied. If it is not clear what kind of data is being requested you should ask the data subject for more information. This could involve identifying the databases, locations or files to be searched or giving a description of the interactions the individual has had with the organisation.
- Log the date of receipt of the valid request.
- If data relating to a third party is involved, do not disclose without the consent of the third party or anonymise such data if this would conceal the identity of the third party.
- Monitor process of responding to the request – observing time limit of one month.

- Supply the data in an intelligible form (include an explanation of terms if necessary).

Recognize that twice a calendar year you shall provide the information to the data subject free of charge.

Where the data subject, after access to his personal data, finds out that information kept about him is incorrect, incomplete or inaccurate and applies to you, you must immediately rectify the data and/or restrict further processing except it is keeping (see Sec. 16 Par. 1). In some circumstances, the data subject may also have the information erased altogether from the database - for example, if you have no legal ground to hold it (i.e. it is irrelevant or excessive for the purpose), or if the information has not been obtained fairly.

Note that the PDP Law sets out a small number of circumstances in which rights of the data subject can be limited.

14. Does the State Data Inspection advise and help me?

The State Data Inspection (SDI) has specific responsibilities for the promotion and enforcement of the PDP Law. Under the PDP Law the SDI shall inter alias:

- examine personal requests and complaints,
- check the lawfulness of personal data processing and take decisions in respect of the breaches of personal data processing and
- provide consultation to system controllers and draw up methodological recommendations on the protection of personal data and make them public on the Internet.

SDI will be happy to provide you further assistance and information.

Contact us:

The State Data Inspection / Datu valsts inspekcija

Kr. Barona 5-4
1050 Riga
Latvia

Tel. 7223131
Fax 7223556
<http://www.dvi.gov.lv>
info@dvi.gov.lv

15. Where I can get more information?

Additional guidance on the PDP Law is available on our website at <http://www.dvi.gov.lv/>.