



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

Document 25

Activity 4.3

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

Data Protection in the Private Sector Brochure

written by

Dr. Philipp Scholz, Gregor Scheja

August 2005



**Ludwig Boltzmann Institut für Menschenrechte
Mandated Body**



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.

Introduction

This is a straightforward guide to following the requirements of the Personal Data Protection Law (PDP Law). It tries to answer system controllers' most frequently asked questions and should be understood as a valuable starting point in helping them to achieve compliance with the PDP Law.

1. What's the Personal Data Protection Law (PDP Law) all about?

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, titled system controllers, while giving rights to those individuals who are the subject of that data.

Processing, in relation to data, means obtaining, 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)

The PDP Law (Sec. 1, 2 No. 3) only protects personal data, that is any information relating to a living individual or a legal person (data subject) who is or can be identified either directly from those data (e.g. name and address) or indirectly from those data in conjunction with other information which is in, or is likely to come into, the possession of the system controller (e.g. personal identity number, bank account number). The term "information" includes also sounds and images (e.g. photos, video). Not only facts are concerned but also assessments relating to an individual. 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.

Example: The disclosure of the current account balance of a deceased person is not covered by the PDP Law. The Law is only concerned with living individuals and so if the subject of the information is dead, then the information cannot be personal data.

Example: Legal persons, such as incorporated or limited companies, are included from the scope of protection. Information about a legal person can include at the same time information relating to a natural person.

Example: Please bear in mind that under certain circumstances also an IP address, which is a unique number used by computers to refer to each other when sending information through the Internet, can be a personally identifying information of the user.

Example: Statistical data itself typically don't relate to a particular person. But the information that someone belongs to a statistical group (e.g. "Credit-Rating") is information relating to a natural person.

2. Am I a System Controller?

It is important to establish whether or not you are a system controller because compliance with the legal obligations in respect of the handling of personal data is the responsibility of the system controller.

System controller signifies a person who (either alone or jointly with other persons) determines the purposes of personal data processing systems and means of processing (Sec. 2 No. 9). In other words the party who decides why personal data is, or will be, held and the way in which such data is, or will be, dealt with. The term 'personal data processing system' embraces every structured body of personal data recorded in any form that is accessible on the basis of relevant person identifying criteria (Sec. 2 No. 5).

A system controller must be a natural or a legal person. This comprises not only individuals but also organizations such as companies and other corporate and unincorporated bodies of persons.

Example: A company that holds personal data that it uses for own business means (e.g. customer addresses) is likely to be a system controller. In contrast a company that received a list of names and addresses from another company (system controller) with instructions to mail out promotional leaflets to the customers on the list is usually not a system controller, because it has not decided why or how the data is processed. In this case the system controller retains full responsibility for the actions of the so called operator of personal data, provided the takeover of the processing is based on a written contract (Sec. 2 No. 6). The PDP Law also introduces specific obligations upon system controllers when the processing of personal data is carried out on their behalf by operators (cf. Sec. 14).

Example: A third party provides a company with IT services, makes available a computer center, takes over the administration of the payroll or serves as call center or collection service.

Personal data are exempt from the scope of the PDP Law where they are processed by a natural person only for the purposes of that individual's purely personal activities (e.g.

family or household), unrelated to business or profession, and where the collected personal data are not disclosed to other persons (Sec. 3 Par. 3*).

Example: If you hold a list of your friends' addresses for private purposes then you are, strictly speaking, a system controller. However, the legal obligations imposed upon system controllers by the PDP Law do not apply where the data is held solely for personal affairs.

Example: If you carry out a private website and publish personal data throughout the world by this means, you are a system controller and have to observe the PDP Law.

The PDP Law shall not apply in so far as the 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 by making use of equipment in the Republic of Latvia, except where such processing is carried out by an establishment in the Republic of Latvia (Sec. 3 Par. 4*).

Example: A German polling institute carries out a survey in the Republic of Latvia, without maintaining any offices, branches or agencies acting on its behalf in the Republic of Latvia and without making use of equipment situated on the territory of the Republic of Latvia. In this case German Data Protection Law applies.

Example: A Latvian data operator processes personal data on behalf of a French company. The legitimacy of the processing is based upon French data protection law.

System controllers established outside of the European Union and the European Economic Area are subject to Latvian data protection law when they make use of equipment in the Republic of Latvia for the purpose of processing personal data. System controllers that are covered by this rule must designate a representative established in the Republic of Latvia. This representative would, in general, be expected to be responsible for compliance with Latvian data protection laws (Sec. 3 Par. 1 No. 3, Par. 2*).

3. Which are the basic principles of data processing?

As a system controller you are required 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

* Amendment to the Personal Data Protection Law, Draft August 2005.

* Amendment to the Personal Data Protection Law, Draft August 2005.

* Amendment to the Personal Data Protection Law, Draft August 2005.

question 4 below). The principle also requires system controllers generally to inform the data subject about the purposes for which the data are intended to be processed (see question 10 below).

Example: Data processing might be unfair and unlawful, if personal data is collected secretly without notifying the data subject.

- collected for specified purposes determined before collecting personal data and are later processed in accordance with the intended purpose and to the extent required therefore;

The purposes which were determined in advance restrict the system controller and the data recipient to process the data in a way which is compatible to the purposes. If you obtain personal data for a particular purpose generally you may not provide the personal data to a third party, except in ways that are "compatible" with the specified purpose. As far as you plan to process personal data for other purposes than intended originally again for the planned processing you have to meet all the criteria for lawful processing set out in the PDP Law.

Example: The marketing division of a company intends to merge all available customer data (contract data, mail order data, billing data, credit information, assurance data, information about complaints, encashment data, etc.) in order to analyse these combined information for direct marketing purposes. Due to the fact that the personal data were collected originally for different and incompatible purposes, the planned processing would be unlawful (unless the data subjects have given their specific and informed consent).

According to this principle, system controllers should also seek to identify the minimum amount of information that is necessary in order properly to fulfil their purpose. If it is necessary to hold additional information about certain individuals, such information should only be collected and recorded as far as necessary.

Example: Many companies issue customer loyalty cards. In this context they usually obtain quite a number of personal customer data, e. g. name, gender, residence, phone number and e-mail address. But often this information is not necessary for the bonus calculation itself. That applies in particular to the Personal Identification Number. This is why the latter should not be obtained.

- 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 anonymize the information which is no longer necessary for the attainment of the intended purposes. If personal data have been recorded because of a relationship between the system controller and the data subject, it should be taken into consideration whether these data should be erased when the relationship ends.

Example: In the case of a contractual relationship it may be necessary to retain certain information to enable the system controller to defend legal claims, which may be made in the future. Unless there is some other reason for keeping them, the personal data should be deleted when the possibility of a claim arising no longer exists i.e. when the relevant statutory time limit has expired.

Example: Business letters have to be archived as long as an audit e.g. by revenue authorities could come up. After termination of the necessary retention period these letters have to be destroyed.

- 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.

Example: Customer databases have to be updated regularly. Credit scores have to reflect the actual state of affairs. In practice it might be a good solution to record the date of validation of personal data as well to guarantee accuracy.

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

In the private sector at least one of the following conditions (cf. Sec. 7) must be met for personal data to be considered lawfully processed (except where it is prescribed otherwise by law):

- the data subject has consented to the processing;
- processing results from contractual obligations of the data subject or processing is necessary for the conclusion or performance of a contract with the data subject;
- processing is necessary for compliance with a legal obligation (other than one imposed by the contract) to which the system controller is subject;
- processing is necessary in order to protect the vital interests of the individual, including life and health;
- processing is necessary in order to pursue the legitimate interests of the system controller or third parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.

One alternative for lawful processing is that the data subject has given his/her consent to the processing. Under the terms of the PDP Law the data subject's consent is defined as any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to the processing of personal data relating to him (Sec. 2 No. 2).

The fact that the data subject must "signify" his/her agreement means that there must be some communication between the parties.

Example: System controllers cannot infer consent from non-response to a communication, for example from a customer's failure to return or respond to a leaflet.

A data subject may “signify” agreement other than in writing.

Example: On the Internet an electronically consent can be sufficient.

A consent is only legally effective if it is a freely given indication.

Example: The data subject is obviously not free to give or deny a consent, if he is in a social relationship of dependence – like in an employment contract – or if the consent is combined with needs or benefits to which the data subject depends existentially.

Example: In order to grant a real choice between consent and no-consent it should be provided a ‘yes’ and a ‘no’ check box in the contract forms. An “Opt out” as the necessity to object against the processing not 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 data recipients. As a result vague and generalized consent clauses are inadequate.

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 may withdraw the previously given consent.

As mentioned above personal data may be lawfully processed as well, if a contract to which the data subject is a party is being concluded or performed.

Example: Please examine with minuteness what customer data you essentially need before setting your contract forms. Note that you have to specify the purpose or purposes for which the personal data are obtained. When the customer is asked to fill in contract forms, there distinction between voluntary and obligatory parts of the requested information could be made.

5. Are there specific conditions for processing sensitive data?

Yes, specific provision is made under the PDP Law 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). For such data to be considered lawfully processed, at least one of the following conditions must be met (cf. Sec. 11*):

- the data subject has given his/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.

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. Correspondingly trade unions have to keep member data in confidence.

6. Do you intend to disclose personal data to a data recipient?

If so, this is only lawful on the basis of a written application or agreement, if not prescribed otherwise by law (Sec. 13 Par. 2). The declaration has to 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.

Example: Note that transfers of personal data to agents of yours, who are carrying out operations upon the data on your behalf and not retaining it for their own purposes based on a written contract, do not constitute "disclosure" of data for the purposes of the Law.

Please notice that you could be obliged to disclose personal data to officials of State and local government institutions in cases provided by law.

* Amendment to the Personal Data Protection Law, Draft August 2005.

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

Transfers of personal data to foreign countries which are non-member states of the European Union shall in principle be subject to an authorisation from the Data State Inspectorate (DSI). If there is an adequate level of data protection in these countries the DSI has no latitude to withhold authorization. An authorization to transfer personal data to a third country without a generally adequate level of protection may be granted (in so far as the DSI has latitude) by the DSI if adequacy is ensured by contractual or self-regulatory means.*

An authorization by the DSI is not necessary only if

- the data subject has given his unambiguously consent to the data export, or

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;

Example: A person in the Republic of Latvia buys some software from an US seller by using a web shop. The transmission of the data subject's name, address and possibly credit card number or bank account information by the web shop to the US seller might be required to fulfil an agreement between the data subject and the system controller.

Example: A person in the Republic of Latvia buys a world trip via a travel agency. To organize the trip the agency transmits personal data of the traveller to car rental services, airlines, and hotels in numerous non EU-countries.

- the data transfer is necessary or provided by law for an important public interest or for the purpose of legal proceedings in court,

Example: A system controller in the Republic of Latvia is involved as a party in legal proceedings in a third country and needs to make personal data available in that third country for the purpose of the legal proceedings.

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

* For further information cf. the European Commission's website at http://europa.eu.int/comm/justice_home/fsj/privacy/modelcontracts/index_en.htm.

Example: A sudden illness of the data subject makes international transfer of relevant data necessary. 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 – this provision should be invoked.

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

Example: As far as the data subject published personal data in the Internet by him/herself, these data might be transmitted to non EU-countries by third parties. Data from a public telephone book might be used as well.

8. Why should I comply with the PDP Law?

Firstly because it is a legal requirement and serious sanctions might occur in case of non-compliance.

However, it also makes good business sense.

Example: A high level of data protection can enhance your business's reputation by increasing customer and employee confidence in you.

Example: Good information handling should reduce the risk of a complaint being made against you.

Example: If you are not in line with data protection requirements, and an individual suffers damage as a result, then that individual may also seek compensation for the damage through the courts.

9. What happens if I don't comply?

Your business's reputation and finances could be affected.

The Data State Inspectorate (DSI) could also take enforcement actions against you 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).

10. What do I actually have to do?

- Informing the Data Subject

The precondition of legitimate processing of an individual's data is that the data subject is informed about the fact that data processing is being carried out (Sec. 8). When data are obtained directly from the data subject and applicable law does not exclude the necessity to inform the data subject, 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.

At request of the data subject the information should also comprise:

-
- data recipients and purposes of the providing,
- 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: After buying a sofa the customer wishes to be supplied with the furniture. If the furniture store mandates a carrier, the customer has not to be informed about the disclosure of the address data towards the carrier in advance, because transmission of the address data to a carrier and purpose of this transmission are obvious for the data subject. The identity of the carrier becomes obvious for the data subject when carrier approaches.

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 (unless one of the exceptions of the PDP Law applies). In addition to the information mentioned above you have to inform the data subject about the categories and sources of the personal data which are being collected or will be collected (Sec. 9).

Example: A mail order company obtains names and addresses from a list broker. He stores this information in his customer data base. Thus he has to provide to the data subjects amongst others the source of the 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. In circumstances where you have obtained data from someone other than the data subject, the fair processing information must be given to the data subject before the time when you first process the data, or in a case where you intend to disclose data to a third party not later than at the time when the data are first disclosed to a third party.

Example: Note the information is not demanded when the data subject already knows about the processing of his personal data.

- Notifying on data processing by automated means

Quite often registration to the Data State Inspectorate (DSI) by a private company is not necessary because of relative extensive exemptions in Sec. 21 Par. 3*. Exceptions are provided for cases, when the data subject may obtain the data relating to him/her, and furthermore, either 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 11 below).

But still under specific circumstances system controllers have to let the Data State Inspectorate know certain details about themselves including the types of information they hold and the purposes for which they process personal data (Sec.21, 22). The DSI examines this notification with regard to the observance of personal data protection provisions and decides whether a personal data processing operation has to be registered. Where this is the case, the DSI 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 specific system controllers – maintained by the DSI – is transparency or openness. The public should know or should be able to find out what kind of data processing is carried out by these specific system controllers.

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.

* Amendment to the Personal Data Protection Law, Draft August 2005.

* Amendment to the Personal Data Protection Law, Draft August 2005.

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

- 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 DSI. If no data protection official has been appointed, the DSI itself is obliged to carry out the prior checking. In all these cases the data controller has to notify the DSI 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 Law (Sec. 25) requires the system controller and a possible data operator 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.

* Amendment to the Personal Data Protection Law, Draft August 2005.

* Amendment to the Personal Data Protection Law, Draft August 2005.

* Amendment to the Personal Data Protection Law, Draft August 2005.

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 have to 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 operator 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).

11. Should I appoint a data protection official?

The establishment of data protection officers by companies is a modern development in many companies around the world. 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 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, France, Slovakia, The Netherlands).

According to Sec. 23 (1) public and private bodies processing personal data may appoint in writing a data protection official (DPO). Therefore appointing of a DPO is just an option for the system controller. 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 Data Supervisor. That's the background why the DPO may consult the Data Supervisor at any time (Sec. 23 (7)), e.g. in case of doubt or of conflicts with the system controller. The establishment of a DPO is a classic example for self regulation in the private sector. A considerable advantage of appointing a DPO is that the system controller does not have to notify its data processing activities to the Data Supervisor anymore (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 public or private body. 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/her function. The DPO shall report directly to the board of directors or the head of the company.

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))
- carry out prior checkings (Sec. 22b*)
- 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 legally compliance of the data processing activities of the system controller and to carry out specific training of employees in data protection issues. Training of employees and promotion of awareness can also be made by sending appropriate e mails 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 maintain knowledgeable. Serious 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 him/herself liable to prosecution the necessary reliability for performing this function may disappear. Also violation of confidentiality (Sec. 23 (4)) might destroy reliability.

The DPO shall not be exposed to any conflict of interests with regard to other duties by reason of his appointment (Sec. 23 (2)). Therefore members of a board of directors or the head of a company and the managing director of the HR department as well as the IT department should not be appointed as DPO.

A person from outside a body concerned 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 anymore. External DPOs can give valuable advise to handle data protection issues in a striking and cost-effective way.

Data subjects may approach the data protection official at any time by maintenance of fully confidentiality (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, furnishings, 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.

* Amendment to the Personal Data Protection Law, Draft August 2005.

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/>.

12. 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/her 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 billing purposes: name: John Q. Customer; bank details: 1234567, etc."

about the information has to consider 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.

Example: 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.

You must comply with a data subject access request promptly, in other words as quickly as you can, and in any event within one month of receipt of the request. On inquiry information must be provided to the data subject in written form.

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

- Appoint a coordinator who will be responsible for the response to the access request. All subject access matters should be submitted to the coordinator. The data privacy officer should be appointed if there is any.
- 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).

Where the data subject, after access to his personal data, finds out that information kept about him is incorrect, incomplete or inaccurate, the system controller must immediately rectify the data and/or restrict further processing (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.

13. Does the Data State Inspectorate advise and help me?

The Data State Inspectorate (DSI) has specific responsibilities for the promotion and enforcement of the PDP Law. Under the PDP Law the DSI 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.

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

Contact us:

The State Data Inspectorate / Datu valsts inspekcija

Kr. Barona 5-4
1050 Riga
Latvia

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

14. Where I can get more information?

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