Twinning project "Implementation of the best European practices with the aim of strengthening the institutional capacity of the apparatus of the Ukrainian Parliament Commissioner for human rights to protect human rights and freedoms (apparatus)"
No. EuropeAid/137673/DD/ACT/UA

Activity 2.1.4. Developing new or improving the existing methodologies and procedures to carry out a monitoring of the observance of human rights, ensuring activities of the Ombudsperson in preventing such violations

Document	Methodology for Evaluation of Draft Legal Acts from the Perspective of Personal Data Protection
Short description of the document	This Methodology suggests the requirements for the content of the conclusions on draft legal acts that are prepared by the Personal Data Protection Department. It offers guidelines for employees of the Department useful when drafting such conclusions and provides practical advice on aspects that should be considered when evaluating draft legal acts. In addition, some examples of good practice are included.
Author	Danguolė Morkunienė, Agnė Limantė
Date	December 2017, Kyiv

METHODOLOGY FOR EVALUATION OF DRAFT LEGAL ACTS FROM THE PERSPECTIVE OF PERSONAL DATA PROTECTION

Table of contents

1. INTRODUCTION

Article 3 of the Law of Ukraine on the Ukrainian Parliament Commissioner for Human Rights foresees that facilitation of the process of bringing legislation of Ukraine on human and citizens' rights and freedoms in accordance with the Constitution of Ukraine and international standards in this area is one of the purposes of the parliamentary control over the observance of constitutional human and citizens' rights and freedoms. According to the Article 23 (1) (8) of the Law of Ukraine on Personal Data Protection, the Ukrainian Parliament Commissioner for Human Rights (hereinafter – the Commissioner) is empowered to submit proposals to the Verkhovna Rada of Ukraine, the President of Ukraine, the Cabinet of Ministers of Ukraine, other state bodies, bodies of local self-government and their officials as regards the adoption or amendment to normative legal acts on the protection of personal data.

Methodology for the Evaluation of Draft Legal Acts from the Perspective of Personal Data Protection (hereinafter – the Methodology) sets the requirements for the content of the conclusions that are prepared by the Personal Data Protection Department on draft legal acts (hereinafter – the Conclusions) and guidelines for employees of the Personal Data Protection Department when drafting such Conclusions. It also provides practical advice on aspects that should be considered when evaluating draft legal acts and gives some examples of good practice.

2. GENERAL OBSERVATIONS REGARDING EVALUATION OF DRAFT LEGAL ACTS

It is very important that when drafting legal acts, the quality of the content is ensured. Personal data protection is one of the areas that should be given a specific attention. In this context, the Personal Data Protection Department serves as a body providing its expertise in the area of personal data protection. When preparing Conclusions, the following aspects should be assessed and evaluated:

- Whether the regulation foreseen in the draft legal act is in compliance with the provisions of national and international legislation in personal data protection field, as well as with regard to the doctrine of law, international guidelines and national and international case-law (in particular the case law of the European Court of Human Rights and the Court of Justice of the European Union; see Section 4 as to the references to case law). This is particularly important in order to ensure the quality of the Conclusions of the Commissioner; moreover, this gives bigger credibility to the Conclusions and increases the chance that the drafter of the legal act will take the comments into account.

- Whether the legislative body is competent to adopt such kind of legal act regulating particular matters, paying specific attention to secondary legislation. This is important in order to ensure that there would be no unlawful ground to process personal data.

- Whether the regulation proposed is not in contradiction or in competition with already existing legislation. In case it is established that the proposed regulation is in contradiction or in competition with already existing legislation, it is necessary to highlight this in the Conclusions. This is essential in order to ensure consistent legal framework of data protection:
  - In case there is an inconsistency between the draft legal act and a higher legal act, the provisions of the draft should be amended respectively.
  - In case there is an inconsistency between the draft legal act and a legal act of the same level, it is necessary to identify which of the regulation will have priority.

- Not only the draft of the legal act itself, but also supporting documents (explanatory memorandum, etc.) should be evaluated. Usually these documents contain information that is especially important with regard to intended regulation, for example, explaining why such volume of personal data is necessary; on the other hand, provisions of these supporting documents can also be subject to evaluation.

It is recommended that all the unclear points, doubts and their reasons should be explained in more detail. When giving comments in the Conclusions, it is recommended to offer suggestions as to improvements; in case where inaccuracies in the legal drafting are indicated, it is advisable to provide alternative formulations.

- When preparing the Conclusions, the following necessary aspects should be taken into account:
  - Object and legal basis of the draft;

- what is the objective of the legal regulation;
- is it defined precisely and unambiguously;
- is it necessary to change the legal regulation in order to achieve the objective, etc.

- Regulatory measures established;

- whether the chosen regulatory measures are proportionate to the objective and could help to achieve it;
- whether there are no other regulatory measures that could achieve the objective of legal regulation more efficiently and economically;
- whether the regulatory measures are proportionate to the objective pursued and are necessary for the improvement of legal regulation;
- whether the objective of the proposed regulation could not be achieved by measures imposing fewer restrictions, obligations or prohibitions, etc.

- Possible effects;

- if the requirements are made stricter – whether this is proportionate to the objective pursued;
- whether the adoption of the draft would not create contradictions of legal norms (legal regulation) or competition of them; whether the regulatory framework would remain consistent, and not-contradictory;
- whether relevant timeframe has been foreseen for the introduction of legal regulation (for example, whether the time-limit for entry into force of the act is such as to allow for proper preparation for the implementation of the law);
- whether the implementation of regulatory measures would not cause negative consequences for individual entities or their groups, etc.

- Legal drafting;

- whether the text of the draft legal act is understandable, clear, unambiguous, and in line with personal data protection principles;
- whether the terminology used in the draft legal act is in line with the terminology used in the legal acts regulating personal data protection;
- whether the draft legal act contains precise references to legislation, etc.

The Conclusions should list motivated comments on shortcomings relating to all relevant aspects mentioned above. This is important to guarantee the consistent legal framework in personal data protection and legal certainty of the addressee of the Conclusions as to conformity of all the draft legal act with the requirements of personal data protections principles.

- Other aspects that, in the opinion of the employee preparing the Conclusions, are important in the respective situation.

3. AS TO REQUIREMENTS TO DRAFT LEGAL ACTS UNDER THE GDPR

Article 6 (1) of the Law of Ukraine on Personal Data Protection foresees that the purpose of personal data processing must be clearly formulated in laws and other subordinate legislation, regulations, constitutive or other documents that regulate activity of the controller of personal data, and should conform to legislation on personal data protection. In such a way, the Law of Ukraine on Personal Data Protection sets forth clear obligation for legislative bodies on which the Commissioner could rely when giving Conclusions on the drafts of legal acts.

When drafting the Conclusions, it is recommended to take into account the provisions of the GDPR[1] which establish the requirements for legal acts that are setting the legal basis for the processing of personal data.

Under Article 6 (3) of the GDPR, that legal basis:

- should establish the purpose of processing of personal data;
- could set specific provisions regulating the lawfulness of the data processing performed by the data controller.

The lawfulness of the processing of data by the data controller can be assessed if, in addition to the purpose of processing of personal data, the draft legal act identifies:

- the types of data which are subject to the processing;
- the data subjects concerned;
- the entities to, and the purposes for which, the personal data may be disclosed;
- the purpose limitation;
- storage periods; and
- processing operations and processing procedures, including measures to ensure lawful and

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

fair processing.

When drafting the Conclusions on draft legal act which provides for processing of sensitive personal data (the GDPR specifies such data as special category data), in specific case (Article 9 (2) (b), (g), (h), (i), (j) of the GDPR), it must be assessed whether the draft legal act[2]:

- envisages regulation that is proportionate to the aim pursued;
- respects the essence of the right to data protection;
- provides for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
- sets the obligation of professional secrecy.

4. AS TO THE JURISPRUDENCE OF THE COURT OF JUSTICE OF THE EUROPEAN UNION AND THE EUROPEAN COURT OF HUMAN RIGHTS

In certain cases when drafting the Conclusions, it is particularly advisable to refer to the jurisprudence of the Court of Justice of the European Union and the European Court of Human Rights. Below are several examples to specific questions:

- **When ensuring a person's right of access to his/her personal data, is the data controller obliged to provide the person with copies of documents in which his/her personal data have been processed?**

In its judgment of 17 July 2014 in Joined Cases C-141/12 and C-372/12, the Court of Justice of the European Union noted that „<...> in so far as the objective pursued by that right of access may be fully satisfied by another form of communication, the data subject cannot derive from either Article 12(a) of Directive 95/46 or Article 8(2) of the Charter the right to obtain a copy of the document or the original file in which those data appear. In order to avoid giving the data subject access to information other than the personal data relating to him, he may obtain a copy of the document or the original file in which that other information has been redacted".

- **Is publication of personal data on a website an interference with private life?**

[2] See GDPR, Article 9 (2).

In its judgment of 9 November 2010 in Joined Cases C-92/09 and C-93/09, the Court of Justice of the European Union noted that because the information becomes available to third parties, publication on a website of data with personal names constitutes an interference with private life. The Court has also held in this judgement that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary. Furthermore, the Court stated that the institutions are obliged to balance, before disclosing information relating to a natural person, the European Union's interest in guaranteeing the transparency of its actions and the infringement of the rights recognised by Articles 7 and 8 of the Charter. They should take into consideration methods of publishing information on the beneficiaries concerned which would be consistent with the objective of such publication while at the same time causing less interference with those beneficiaries' right to respect for their private life in general and to protection of their personal data in particular, such as limiting the publication of data by name relating to those beneficiaries according to the periods for which they received aid, or the frequency or nature and amount of aid received. No automatic priority can be conferred on the objective of transparency over the right to protection of personal data, even if important economic interests are at stake.

- **What are the requirements for legal acts that restrict human rights?**

It is recommended that a measure that imposes an obligation to process personal data would be in line with the case law of the Court of Justice of the European Union and the European Court of Human Rights.

To assess whether a state has legally interfered with someone's human rights, the European Court of Human Rights has generally held that there are three conditions that should be met. The restriction (i) must be prescribed by law, (ii) it must pursue a legitimate aim, and (iii) it must be necessary and proportionate to pursue that aim. The restrictions prescribed by law should also be sufficiently precise and accessible to public.

As for the type of legal act, first of all the national law should be analysed. In accordance with the Article 22 of the Constitution of Ukraine, the content and scope of the existing human rights and freedoms that are provided by the Constitution shall not be diminished by an adoption of new laws or by introducing amendments to the effective laws. Under Article 32 of the Constitution, no one shall

be subjected to interference in his private life and family matters, except when such interference is stipulated by the Constitution of Ukraine. The collection, storage, use, and dissemination of confidential information about a person without his consent shall not be permitted, except for the cases determined by law and only in the interests of national security, economic welfare, and human rights.

Furthermore, the content of the legal acts is also very important as well as the fact whether the legal act is published for the society to be able to access it. From this perspective, the case law of the European Court of Human Rights is important.

The case of *Shimovolos v. Russia* (application No. 30194/09) which was analysed by the European Court of Human Rights should be reminded here. The case concerned the registration of a human rights activist in the so-called "surveillance database", which collected information about his movements, by train or air, within Russia, and his arrest. The creation and maintenance of the database and the procedure for its operation were governed by a ministerial order which had never been published or otherwise made accessible to the public.

The European Court of Human Rights reminded that under its case-law, the expression "in accordance with the law" within the meaning of Article 8 (2) requires, firstly, that the measure should have some basis in domestic law; it also refers to the quality of the law in question, requiring it to be accessible to the person concerned, who must, moreover, be able to foresee its consequences for him.

Thus, in order for that interference to be justified, minimum safeguards had to be set out in statute law to avoid abuse. The database in which Mr Shimovolos' name had been registered had been created on the basis of a ministerial order which had not been published and was not accessible to the public. Therefore, people could not know why individuals were registered in it, for how long information was being kept about them, what type of information was included, how the information was stored and used and who had control over that. As a result, the scope and manner of collecting and using the data in the surveillance database had been neither clear, nor foreseeable, contrary to the requirements of the ECHR and in violation of Article 8.

5. AS TO COOPERATION WITH OTHER ENTITIES (ACTIONS TO BE TAKEN IN ORDER TO ENSURE QUALITY OF THE CONCLUSIONS)

In cases where the employee preparing Conclusions has some questions or doubts as to the objective or the legal basis of regulation proposed, means to achieve the objective or other issues provided in the draft, he/she should make use of all the available options to clarify the situation (e.g. contact the drafters of the draft legal act, analyse existing legislation relating to the matter, etc.).

In case the draft legal act covers areas falling within the competence of other departments of Apparatus (for example, access to public information), the opinion of civil servants of particular department should be sought (this is important for ensuring the consistency and continuity of process of evaluation of drafts legal acts and trust in the Commissioner).

It is recommended to establish internal procedure regulating interaction between structural units of Apparatus of the Commissioner, time limits and other aspects related to drafting of Conclusions.

6. REGARDING TIME LIMITS FOR EVALUATION OF DRAFT LEGAL ACTS

It is important to note that in case where in national legal acts no time limits for evaluating or re-evaluating draft legal acts are established, it is recommended for the Commissioner to have the deadlines set internally. For example:

- The Conclusions should be presented not later that within 10 working days. In case of drafts longer than 10 pages and/or complex drafts of legal acts (establishing new regulation or materially changing the present regulation), the Conclusions should be presented not later that within 15 working days.

- If due to the urgency of the situation, the draft legal act should be adopted with no delay, the Conclusions should be presented not later than within 5 working days.

- The time limit to present the Conclusions starts the next working day after the receipt of the draft legal act.

7. REGARDING TYPICAL SHORTCOMINGS APPEARING IN DRAFT LEGAL ACTS

When analysing the draft legal acts, it is important to remember that typically the following shortcomings related to personal data protection and protection of privacy appear:

- It is incorrectly established what should be considered as personal data:
  - ➢ It is established that an institution will publish on its website open data (as it is defined in the EU directive on the re-use of public sector information (Directive 2003/98/EC[3]), however, the data in question should be seen as personal data;
  - ➢ It is established that no personal data will be made public, however, from the provisions of the draft legal act it is clear that publication of personal data will appear.

Example 1

„Department (state institution) may publish information about the experts after having depersonalized them. Information about expert contacts can be used to compile lists of persons to be invited for the events organized by the Ministry.“ (extract from the draft law)

It is not clear from this provision:

- what information about experts should be considered as personal information that needs to be depersonalized (this could be unclear to persons who will be assigned with a duty of implementing the provision);
- whether from such depersonalized information it will not be possible to identify the expert either directly or indirectly;
- where and for how long such information will be made available to the public, i.e. whether this information will be published on the institution's website or by other means.

Suggested:

[3]As amended by the Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013.

- In draft legal acts, when providing for the publication of certain depersonalized information, it is advisable to indicate what data is considered to be depersonalized information.

Example 2

„ The Territorial Labour Exchange, if requested by a social enterprise, shall provide information about registered individuals who belong to specific target groups.“ (extract from the draft law)

It is not clear from this provision:

- for what purpose of personal data processing and what types of personal data should be provided by the Territorial Labour Exchange, and whether provision of personal data is necessary at all – perhaps depersonalized information is sufficient;
- if provision of personal data is necessary, under which procedure should it be provided.

Suggested:

- where a legal act provides for the obligation to provide personal data, it should also define what types of personal data must be provided; it is not proper simply to name it “information” (there should be no doubt as to whether such data should also include personal data);
- to establish the procedure for the provision of personal data (reference may be made to the legal act regulating this).

- The draft legal act provides for unjustified publication of personal data:
  - there might be the case of absence of the legitimate purpose of processing of personal data; or
  - when the processing of such data is established by a legal act of too low level.

- The purpose of processing of personal data is not clearly defined.

Example 3

„ For the purposes of implementing the Program of Official Statistics, the institutions assigned

with the task of managing official statistics have the right to obtain, free of charge, contact details of physical and/or legal persons (addresses, fixed and mobile telephone numbers, e-mail addresses). (extract from the draft law)

It is not clear from this provision:

- objectives to attain which personal data is needed;
- the sources from which these contact details will be received (such data providers are not required to provide this data).

Suggested:

In assessing draft legal acts that provide for the right of public authorities to obtain personal data, it is suggested to request to supplement this provision by defining:

- objectives to attain which personal data is needed;
- the sources from which these contact details will be received and to establish the duty of data providers to provide such data.

Example 4

„The list of persons who have successfully passed the broker exams is published on the supervisory authority's website and is managed in accordance with the procedure established by the supervisory authority.“ (extract from the draft law)

It is not clear from this provision:

- the purpose for which this personal data is made available to public;
- what types of personal data should be included in the publicly available list.

Suggested:

- even if a more detailed procedure on how such data should be published is planned to be defined in a secondary legal act, the law establishing an obligation to publish personal data should at least specify the purposes of the public disclosure of personal data and should specify what personal data will be publicly disclosed.

- The draft legal act provides for processing of excessive personal data. The typical examples could be:
  - ➢ unjustified handling of copies of identity documents;
  - ➢ a draft legal act provides for creation of various state registers and information systems without a legal basis or need;
  - ➢ a draft legal act provides for repeated (duplicated) processing of the same personal data in different registers or information systems for the same purposes of personal data processing;

Example 5

„ Persons who have committed sexual offenses are registered in the Register of Sex Offenders, the controller of which is the Ministry of the Interior. The data of the Register of Sex Offenders is made public.“ (extract from the draft law)

It is not clear from this provision:

- for what purposes such register should be established and what is the need of it as (in Lithuania) similar data on all valid convictions are accumulated and processed in the Register of Suspects, Accused Persons and Convicts. This would amount to a re-processing of the same data;
- why, from the perspective of data processing, it is necessary to make such data public, i.e. proportionality should be evaluated.

Suggested:

- to refrain from establishment of the Register of Sex Offenders in the absence of the legitimate aim of processing personal data;
- in case there is a need to ensure access to the Register of Suspects, Accused Persons and Convicts for a wider range of data recipients, their right to receive such information should be evaluated and the legal acts should be amended accordingly.

  - ➢ a draft legal act provides for unrestricted access to data processed in state registers and information systems, even though personal data processed therein is not public;

➢ a draft legal act provides for access to data processed by registers and information systems for specific recipients, however some of them do not have a legal basis for obtaining and processing such data;

Example 6

„When performing the functions provided for in this law and other legal acts, the Lithuanian Bar Association has the right to obtain (without the consent of the data subject) from state and municipal institutions, state registers, state and municipal information systems, natural and legal persons all the information, data (including sensitive personal data), documents and copies of documents that are needed for performing its functions. (extract from the draft law)

It is not clear from this provision:

- for which particular functions of the Bar would the personal data be obtained for;
- about what types of data subjects would the data be obtained;
- what specific personal data, including sensitive personal data (health or criminal records), would be obtained.

Suggested:

- to define clearly the group of data subjects whose personal data could be obtained by the Bar;
- to define the purpose for which personal data may be collected;
- to assess whether, in certain cases, there should be a right or a duty to receive and process personal data.

➢ a draft legal act provides for unjustified public disclosure of personal data.

Example 7

„In case there is no possibility to inform the debtor about the decision to award him with the benefit, the information about the decision to grant the benefit and the consequences indicated

therein is posted on the Benefit Administrator's website." (extract from the draft law)

It is not clear from this provision:

- for what purpose and what specific information about the decision to grant benefits and the consequences indicated therein would be posted on the Benefit Administrator's website;
- the period for which the information would be published, i.e. it is not clear whether the information would continue to be published after the purpose for which it was published would disappear.

Suggested:

- when evaluating draft legal acts which establish bases for lawful processing of personal data, it should be assessed whether publication of personal data is proportional to the legitimate aim pursued;
- to specify the purpose of the publication of personal data;
- to specify what specific personal data would be published;
- to specify the publication period.

Example 8

„All information and/or documents related to the process of issuing a permit for the provision of passenger transfer services, the declaration, as well as the decision to suspend / revoke the validity of a permit to provide passenger transfer services and other information, shall be made public, except where relevant information and/or documents should not be published." (extract from the draft law)

It is not clear from this provision:

- whether the legal act provides for publication of personal data;
- if one of the purposes was to publish personal data, in such a case the purpose of such publication is not clear;
- what specific personal data should be made public;
- the period for which the personal data would be published.

Suggested:

In draft legal acts that provide for publication of certain information:

- to specify if in making information public certain personal data would also be made public and if so, what specific personal data would be made public;
- to specify the purpose of publication of personal data;
- to specify the period of publication of personal data;
- the legal act which establishes base for processing of personal data – the duty to process personal data, should be concrete and precise, so that it would be clear in what a way and what specific personal data it enables to process.

- The draft legal act provides for the processing of personal data upon the consent of the data subject, however, such consent is not required[4].

Example 9

„The applicant submitting an application to participate in a competition should submit to the the organizing body a consent for the processing of personal data.“ (extract from the draft law)

It is not clear from this provision:

- for what processing of personal data should the applicant express his/her consent;
- whether this consent is an appropriate legal basis for processing of personal data.

Suggested:

- when evaluating draft legal acts, it is advisable that the consent would not be seen as a proper legal basis for processing of personal data in cases where processing of personal data is part of public functions of the data controller.

For example, in case a person would not consent to processing of personal data, he/she will not be able to participate in a competition, thus negative consequences in respect of him/her arise. In such situations, legal acts oblige the state institutions to process the relevant personal data, therefore,

[4]It should be noted that recital 43 of the preamble of GDPR provides that consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation.

consent is not a proper basis for personal data processing.

- The secondary legal act which sets the standard form of certain document(s) provides for unjustified indication of personal identification number, other excessive personal data in the document.

Example 10

„On the front side, the certificate of public servant indicates: the name of the document „Certificate of Public Servant", the coat of arms, the number of the certificate, family name, name (-s), personal identification number, date „valid until", photo." (extract from the regulation of the Government)

It is not clear from this provision:

- for which purpose the drafter of the legal act provided for identification of the personal identification number on the certificate of public servant.

Suggested:

- to remove the identification of the personal identification number from the certificate of public servant as excessive data (instead of personal identification number it is enough to state the number of registration in the Registry of Public Servants, if there is such).

- Other.

Example 11

„For the purposes of this law, when it is necessary to ascertain whether there is a threat to the rights and legitimate interests of the child due to the state of health or conviction of the child's parents or persons living with the child, the Child Rights Protection Service has the right to manage the sensitive personal data related to the conviction and the state of health of the child's parents or persons living together with the child. (extract from the draft law)

It is not clear from this provision:

- what are the specific offenses the data related to which could be handled by the Child Rights Protection Service;

- in what kind of situations, it is considered that the health status of the child's parents, or persons living together with the child may pose a threat to the child's health and safety.

Suggested:

- to assess how the processing of personal data would contribute to the objective pursued, i.e. to assess whether the objective could not be achieved without the handling of specific personal data;
- by envisaging the right of public authorities to process personal data, it should be specified which personal data they have the right to handle; in such a way, it would be ensured that no excessive processing of personal data would appear;
- where a draft legal act establishes an obligation to process personal data, its provisions must be sufficiently clear, so that a person who will be implementing this duty would be sure how the personal data should be processed. A data controller having an obligation to process personal data should not have an unreasonable margin of appreciation to exercise this obligation.

For example, one child rights protection agency might only seek data related to serious and very serious crimes, while others may consider it is necessary to obtain data on all criminal offenses committed; one child rights protection agency might seek data on mental health conditions, while others might think it necessary to obtain data on, for example, infectious diseases.

8. EXAMPLES OF GOOD PRACTICES OF PROVISIONS IN LEGAL ACTS GOVERNING PROCESSING OF PERSONAL DATA

It should be noted that the given examples could be inappropriate in different legal context. For example, the scope of publicly available personal data, as provided in Example 1, in other circumstances may be disproportionate to the pursued objective of the processing of personal data.

Example 1

Article 27 (2) of the Law on Private Detective Activity of the Republic of Lithuania

„For the purpose of ensuring the transparency of the activities of private detectives, the website of the Supervisory Authority provides a list of private detectives operating in the Republic of Lithuania, specifying the following: the name and surname of a private detective, the number of the private detective qualification certificate issued to him, the date of issue, the date of suspension of the validity of this certificate, the date of cancellation of the certificate, the number of the private detective activity certificate, the date of its issue and the date of cancellation. In addition, a list of private detective groups and a list of private detective communities are published on the website of the Supervisory Authority. The Supervisory Authority may also publish on its website other relevant information related to private detective activity, with the exception of personal data. "

It is clear from this provision:

- which institution's website publishes personal information;
- an exhaustive list of personal data that is included in the publicly available list.

Example 2

Article 18 of the Law on Public Health Monitoring of the Republic of Lithuania

„The Ministry of Health of the Republic of Lithuania and its authorized institutions for statistical purposes have the right to process in registries and state information systems personal identification number and special categories of personal data concerning health. The data that was used must immediately be changed so that the identity of the data subject could not be

identified. Personal data included in the data on public health is processed in accordance with the requirements of the Law on Legal Protection of Personal Data of the Republic of Lithuania.

It is clear from this provision:

- purpose of processing of personal data;
- the types of personal data that the authorized authority is entitled to process;
- adequate safeguards are provided, i.e. personal data will only be processed in registers and state information systems (which implies greater protection of such data), and the personal data will be changed immediately.

Example 3

Article 16(9) of Law of the Republic of Lithuania on Prevention of Money Laundering and Terrorist Financing

„A copy of customer's identity document, receipt and/or contractual documentation (original documents) must be kept for 10 years from the end date of transactions or business relations with the customer. Correspondence with the customer on business relations must be kept for 5 years from the date of the transaction or business relationship with the customer in paper or in electronic form. The storage periods may be further extended in cases where the competent authority issues a reasoned order."

It is clear from this provision:

- that there is a right to make a copy of clients' identity documents;
- a specific storage term is set.

Example 4

Article 8 (1) of the Law on Consumer Credit of the Republic of Lithuania

„Before the conclusion of the credit agreement, the creditor must, following the principle of responsible lending, assess the consumer's creditworthiness on the basis of sufficient information, obtained from the consumer and verified by researching in the registers and information databases used for verification of creditworthiness, or by justifying the information

submitted by the consumer on the basis of other proofs.“

In this provision:

- the consumer creditor provider’s right to receive information is clearly established;
- the objective of processing of personal data is clearly defined;
- the provision specifies the sources from which the consumer credit provider has to collect personal data.

Example 5

Article 9 (2) and Article 9 (3) of the Law on Consumer Credit of the Republic of Lithuania

„2. If the credit application is rejected on the basis of information received from the registers and information databases, the consumer credit provider shall inform thereof the consumer immediately and without charge and shall present the information about the registers and information databases which were consulted to assess the consumer’s creditworthiness.

3. The information referred to in paragraph 2 of this Article shall not be provided when the provision of such information is prohibited by other legislation or when it is contrary to objectives of public policy or public security.

This provision:

- establishes the procedure of ensuring the data subject’s right to know about the processing of his/her personal data;
- the law (and not a secondary legal act) lays down restrictions on human rights.

Example 6

Article 13 (1, 3 and 6) of the Law on Intelligence of the Republic of Lithuania

„1. Monitoring of the content of information, correspondence and other personal communications transmitted by electronic communications networks may only be performed on the basis of a reasoned ruling of a regional court. Such actions shall be sanctioned by a reasoned ruling of a judge of a regional court authorised by the chairman of such court under reasoned applications of intelligence institutions.

3. An application of intelligence institutions to a regional court shall contain:

1) data on natural persons (name, surname, personal identification number) or legal persons (address of the registered office, company's number) or objects subject to such actions;

2) data (grounds) substantiating the necessity of carrying out sanctioned actions;

3) data on the terminal equipment to be used to transmit information (identification number, name and/or the location of the terminal equipment);

4) specific actions requested to be carried out and the duration of the requested actions;

5) the result aimed at.

6. The indicated actions may not last longer than six months. When necessary, the time limit for carrying out these actions may be extended for up to additional three months. The number of extensions shall not be restricted. A regional court shall, in each case of extension of an authorisation for the carrying out of actions sanctioned by the court for another three months, assess the grounds for submission of the application for extension of these actions."

These provisions:

- set specific measures for ensuring the rights and freedoms of the data subject (defined actions may be performed only in case they are sanctioned by a court, their duration is limited, the content of the reasoned submission to the court is indicated);
- the law (and not a secondary legal act) lays down restrictions on human rights.