G U I D E
For Personal Data Protection Officers

January 2017

Project funded by the European Union

Project implemented by Consortium led by Vialto Consulting
Project contacts:
18 Goce Delcev Blvd (14th floor)
1000 Skopje
+389 2 3230 635 ext.116

Guide for Personal Data Protection Officers

Publisher

Data protection Directorate

Author

Marijana Marusic Kos

Lecturer

Dijana Ristova

Design and printing

Propoint

Edition

1000 samples

This Guide has been prepared within the project "Support to the Directorate for personal data protection" EuropeAid 135668/IH/SER/MK, financed by the European Union through the IPA TAIB 2012 program and implemented Vialto Consulting Hungary, in cooperation with IPS Institute of Slovenia and the National Authority for Data Protection and freedom of information of Hungary. The views and opinions stated in this Guide do not reflect the official opinion of the European Union.

Table of content

Project funded by the European Union

Project implemented by Consortium led by Vialto Consulting
Project contacts:
18 Goce Delcev Blvd (14th floor)
1000 Skopje
+389 2 3230 635 ext.116

Project funded by the European Union

Project implemented by Consortium led by Vialto Consulting
Project contacts:
18 Goce Delcev Blvd (14th floor)
1000 Skopje
+389 2 3230 635 ext.116

List of abbreviations

DPO – Data protection officer

LPPD – Law on Protection of Personal Data

DPDP – Directorate for Personal Data Protection

WG 29 – Working Group 29

EU – European Union

EC – European Commission

EEC – European Economic Community

Regulation - General regulation on data protection

Project funded by the European Union

Project implemented by Consortium led by Vialto Consulting
Project contacts:
18 Goce Delcev Blvd (14th floor)
1000 Skopje
+389 2 3230 635 ext.116

INTRODUCTION

1. Concept of privacy and personal data protection

Culture for respecting the privacy and protection of personal data is an asset to any democratically developed society, which is being built by valuing basic standards established in the ***United Nations***[1], ***Council of Europe***[2] and the ***European Commission*** (EC)[3] and are elaborated in international and national legal acts relevant for the protection of personal data.

Respecting the right of privacy of the individual is characteristic of more developed countries, which have a long tradition of rule of law and practice of the democracy, but of utmost importance is respecting the right in a social environment that tends toward a higher level of political, legal, economic and cultural living.

With the ***Law on Protection of Personal Data***[4] ***(LPDP)*** which is lex generalis in this area, the right of personal data protection has been incorporated into our legal system that establishes a new concept stressing the importance of this right as one of the fundamental freedoms and right of the individuals and as an essential value of every modern and technologically developed society. This concept involves the privacy and personal integrity of every individual, wherever and whenever personal data are being processed.

Essential for the realization of this concept and establishing higher standards for respecting the privacy is ***appointment of an officer for the protection of personal data*** to the controllers in the public and private sectors, ***a clear definition of his background and job position, respectively relation to the controller, as well as intensifying the cooperation between the controllers and the Directorate for personal data protection (DPDP).***

[1] United Nations - European Convention on Human Rights 1950
[2] European Commission - Directive 95/46 / EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and the free movement of such data, adopted on 24 October 1995, as of May 25, 2018 will replace the Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and the free movement of such data and repealing Directive 95/46 / EC (General Regulation on the protection of personal data) taken on April 27, 2016
General Regulation on the protection of personal data came into force on May 25, 2016, and shall apply from 25 May 2018. It will be legally binding and directly applicable in Member States. Counting from the day you start its application will cease validity of Directive 95/46 / EC
[3] Council of Europe - the Convention on the protection of individuals relating to Automatic Processing of Personal Data of the Council of Europe no.108 / 81
[4] Council of Europe - the Convention on the protection of individuals relating to Automatic Processing of Personal Data of the Council of Europe no.108 / 81

2. Meaning and definitions of the terms used in the Guide

To determine the ***meaning of the terms used in this Guide***, corresponding definitions are taken from LPDP. By defining these terms, the postulates underlying the right to protection of personal data will become clearer and easier to understand the essence and facilitates them in their implementation.

PERSONAL DATA is information that refers to identified physical person or legal entity that can be identified.[5]

PROCESSING means every operation or a number of operations performed on personal data, automatically or otherwise, such as: collection, recording, organizing, storing, adjusting, or altering, withdrawing, consulting, using, publishing through transmitting, revealing or making otherwise available, aligning, combining, blocking, deleting or destroying;

PERSONAL DATA SUBJECT is any natural person to whom the processed data refer;

CONTROLLER is any natural or legal person, a State, or other body, who, independently or with others determines the purposes and the methods of personal data processing;

PERSONAL DATA COLLECTION HANDLER is a natural, a legal person, or a legally authorized state body that could process the personal data on the behalf of the controller;

DATA PROTECTION OFFICER is a person who is authorized by the controller to ensure compliance of the regulations on protection of personal data and to monitor their implementation[6]

CONSENT OF THE PERSONAL DATA SUBJECT is freely and explicitly given statement of will, of the personal data subject whereby he/she agrees to the processing of his/her personal data for previously determined purposes;

SPECIAL CATEGORIES OF PERSONAL DATA (sensitive data) are personal data revealing the racial or ethnic origin, the political views, religious or other beliefs, membership in a trade union and data relating to the health condition, including genetic data, biometrical data or data related to the sexual life.

[5] A person that can be identified is a person whose identity can be determined directly or indirectly, based on the personal identification number or based on one or more characteristics specific to his physical, physiological, mental, economic, cultural or social identity.
[6] In LPDP, there is no definition for the term officer for protection of personal data. The definition is made based on Article 26 of the LPDP.

Project funded by the European Union

Project implemented by Consortium led by Vialto Consulting
Project contacts:
18 Goce Delcev Blvd (14th floor)
1000 Skopje
+389 2 3230 635 ext.116

3. What's the purpose of the Guide and to whom is it intended for?

This Guide ***is intended*** for officers dealing with protection of personal data (DPO) appointed by the controllers[7] in the public and private sectors.

The Guide ***presents*** the role of the DPOs in the Member States countries of the European Union, and in our country, ***inform*** about the obligation to transpose the General Regulation on Data Protection of the European Parliament and of the Council[8] (Regulation) into national legislation, ***elaborate the*** new obligations for the appointing, profiling and position description of the DPO and ***explains*** the tasks of DPO, including key responsibilities of each controller for which fulfilment DPO is responsible.

The purpose of the Guide is to serve as an ***educational and practical tool***:

- ***will clarify*** the relevant provisions of the Regulation[9], which our country has obligation to transpose into national legislation;
- ***will help DPO*** in detail to get acquainted with his role and tasks, as well as with the new job position and responsibilities of the controller after transposition of the Regulation in the national legislation;
- ***will help the controller*** to meets the obligations arising from LPDP and the Regulation, in details, for which fulfilment the responsible person is the DPO;
- ***make recommendations on best practices*** built on already gained experiences in the countries of the European Union (EU), but also at home and
- ***offer more forms of*** acts, reports, plans, lists, tables, records that will help in fulfilling the tasks of DPO and obligations of the controller [10]

[7] In this Guide, any reference to CONTROLLERS applies to PROCESSORS

[8] Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and the free movement of such data and repealing Directive 95/46 / EC (General Regulation on the protection of personal data) is adopted on 27 April 2016. It entered into force on 25 May 2016 and shall apply from 25 May 2018. After the expiry of the transitional period of two years, it will be legally binding and directly applicable in Member States.

[9] Article 37, 38 and 39 of the Regulation

[10] Forms are provided in the appendices to this Guide, are not required to DPO and controllers

Project funded by the European Union

Project implemented by Consortium led by Vialto Consulting
Project contacts:
18 Goce Delcev Blvd (14th floor)
1000 Skopje
+389 2 3230 635 ext.116

MAIN PART

DPOs are balancing between the interest of the controller, subjects whose personal data are protected and the responsibilities imposed by the Directorate.

This is why his role is so specific and delicate, and his new position should be placed in a way that would guarantee independence and prevent political influence in the performance of his duties.

THE MAIN PART of the Guide gives answers on the following questions

- What are the responsibilities of DPO position? [11]
- What obligations are imposed by the Regulation?
- How will be regulated the appointment of new DPO?
- What professional standards must be met by the new DPO?
- What are the tasks of the new DPO?
- What tools will be helpful to strengthen the function of the DPO?

[11] In the Guide the term job position of the DPO is frequently used. This term means a set of tasks of the DPO contained in the LPDP / Regulation and reflected in the act that determines / appointing the DPO and in the job description of the DPO.

4. The current setting of the DPO position

4.1. In EU Member States

Directive 95/46/EC of the European Parliament and the Council, so far, has been a key binding framework which is transposed into national legislation of EU member states.

This Directive ***dose not regulate the DPO position***, and in the absence of regulation that would be the base for a unified approach toward the regulation of this position, ***national laws on the protection of personal data of the EU Member States have their own approach***.

The following is a brief overview about the current regulation of the DPOs positon in EU Member States, until the implementation of the regulation on 25 May 2018.

The national laws of some EU Member States are governing the appointment of the DPO[12], and national laws of other EU Member States do not regulate this position[13]. Some of them, advocate an obligation for controllers to appoint DPO[14], and some of them are engaged on a voluntary base[15]. Some are defining the profile, position and responsibilities of DPO. Thereby, it can be concluded that each national law introduce specifics in their definition. But despite specifics incorporated in the national laws, for fulfilment of this position, essential requirements are as follow:

- appropriate expertise and confidentiality during task performance,
- independence in the implementation of duties,[16]
- ensuring compliance of the controller work with national law on protection of personal data and relevant provisions in other regulations.

4.2. In our country

Current LPDP is more advanced in regulating this position compared with the national laws of some Member States. LPDP regulates this position with Article 26-a. In accordance with this provision, the rule is: mandatory determination of the DPO for the controllers in public and private sectors, with the exception from this obligation for the controller who processes personal data that are part of publicly accessible collections and controller whose collection of personal data apply for up to ten employees or the processing relates to personal data of members of associations based on political, philosophical, religious or trade union objectives. The exemption applies to a controller that processes only publicly available collections, and dose not process other collections of personal data or controller whose collection is for up to ten employees, while no other collections of personal data established for political, philosophical, religious or trade purposes, and if it is processing only the collection of its own members. In practice, very few controllers can come under the legally prescribed exception, therefore the exemption is hardly applicable.

[12] Example: Federal Republic of Germany, the French Republic, the Netherlands, Hungary, Poland, the Republic of Croatia
[13] Example: Federal Republic of Germany, the French Republic, the Netherlands, Hungary, Poland, the Republic of Croatia
[14] Example: Federal Republic of Germany, the Republic of Croatia
[15]Example: Netherlands. The Law on Personal Data Protection of Hungary, the appointment of the officer on a voluntary basis is set out as a rule and mandatory appointment as an exception.
[16] The independence of the officer is reached through the same parameters: providing the necessary resources to perform the function, disabling to suffer from any influence or consequences for performing the functions from the position direct responsibilities in front of highest levels of management of the controller where it is assigned.

Based on the conducted interviews/short survey along with a questionnaire and discussions with the DPO from the public and private sector, deployed in nine focus groups ***it was prepared*** an analyse that identifies some differences between the legal provision that regulates this position and the actual implementation, and discrepancies between the needs and requirements of the DPO and their real functioning, ***which leads to the conclusion that more controllers are aiming to meet the statutory form, not essential to the implementation of the provision, which would involve exercise of the right for protection of personal data.***

The analysis shows that controllers in the public and private sectors have a designate/appoint the DPO, but in some cases the controllers are appointed only formally and to fulfil the legal obligation and not to establish real protection of personal data. Very often, this feature is formally granted to employees who perform other duties in their full-time work. Sometimes, these working tasks are in conflict with the tasks arising from the job position of the DPO.

Current LPDP establishes the tasks[17] of the DPO, but does not identify his profile, or dose not prescribed his professional qualities and experts knowledge, or how his position should be set, nor prescribes minimum standards relating to its status in a way that would ensure its independence.

DPO have established regular cooperation with the Directorate which consists of providing support by the Directorate on matters related to the execution of their office, sharing of information and other communications. The cooperation with the Directorate allows easier compliance with regulations in this area. DPOs will participate in trainings organized by the Directorate and these trainings are not considered only as a method of deepening and upgrading the expert's knowledge, but also as another form for reinforcement and cooperation with the Directorate.

5. What kind of obligations are imposed by the Regulation?

5.1. For EU member states

In an era of globalization[18] and rapid development of information technology for achieving the business cooperation beyond the borders of each State, of ***crucial importance is the consistency of the regulations*** governing the protection of personal data, not only for the institutions and the business community, but also for individuals.

[17] The tasks of the DPO are exhaustively listed in Article 26-a: participate in decision-making process related to the processing of personal data and the exercise of the rights of personal data subjects; follow the compliance with the Law and the regulations made stipulating from the Law concerning the processing of personal data and the internal regulations for the protection of personal data and documentation for technical and organizational measures to ensure confidentiality and protection of personal data; drafting internal regulations for the protection of personal data and documentation for technical and organizational measures to ensure confidentiality and protection of personal data; coordinate control procedures and guidelines set out in the internal regulations on protection of personal data and documentation of technical and organizational measures to ensure confidentiality and protection of personal data; providing training for the employees regarding the protection of personal data and performs other duties prescribed by law and regulations adopted under from the Law, and the internal regulations for the protection of personal data and documentation for technical and organizational measures to ensure confidentiality and protection the processing of personal data.

[18] Initiate bilateral cooperation regarding freedom of institutions, the business community and individuals between two countries.

Project funded by the European Union
Project implemented by Consortium led by Vialto Consulting
Project contacts:
18 Goce Delcev Blvd (14th floor)
1000 Skopje
+389 2 3230 635 ext.116

With the entry into force of the Regulation of 25 May 2016, ***the EU member states started the process of implementation of the provisions that regulates the position of DPO in detail and uniformly.***

Regulation should not be transposed into the national legislation of EU member states. It is legally binding and directly applicable in all Member States. This means that after the expiry of the transitional period of two years, with the implementation, the provisions governing the appointing of the DPO, profiling, as well as description of the DPOs tasks necessarily need to be implemented in all EU Member States; and the provisions from the national law of the EU member states that are inconsistent with the terms, to be determined. Thorough and uniform regulation of the role and tasks of DPO in all EU Member States, will certainly provide an enhancement of his position.

DPO will become a key figure through which the controller will provide and justify but will also demonstrate the compliance of its operations with the regulations on protection of personal data

On December 13, 2016, the Working group 29[19] (WG 29) adopted the ***"Guidelines for officers on protection of personal data"*** with main objective to clarify the section 4 or Articles 37, 38 and 39 of the Regulation, which will help controllers in all EU Member States easier implementation. The most relevant clarifications and recommendations of these guidelines are set out in this Guide.

5.2. For our country

Our country as a candidate country for a membership in the EU, or a country waiting for a date to start accession negotiations for EU integration, has an obligation to transpose the legislation into national law and implement it in the practice. ***The obligation for its transposition should be completed soon, and the new legal solution should forecast a transitional period of at least one year for starting the implementation of the transposed provisions.***

[19] WG 29 is formed on the basis of Article 29 of Directive 95/46 / EC of the European Parliament and the Council. It is composed of representatives from the supervisory authorities for the protection of personal data of each EU Member State, representatives of the European supervisor for data protection and EC officials. In the frames of their authorities, WG 29 provides advice to Member States on issues related to protection of personal data, provides opinions of EC laws concerning the protection of personal data and on its own initiative provide opinions and recommendations on issues related to protection of individuals in the processing of their personal information within the EU. Since June 2007, the Directorate has observer status in WG29.

Project funded by the European Union
Project implemented by Consortium led by Vialto Consulting
Project contacts:
18 Goce Delcev Blvd (14th floor)
1000 Skopje
+389 2 3230 635 ext.116

6. How is going to be regulated the appointment of the DPO?

Regulation provides which controllers will be obliged to elect DPO, who can be appointed as DPO and option for one appointed DPO to carry out the function for more than one controller will be given.

In addition, the provision of the Regulation for the appointment of DPO[20] is elaborated with explanations and recommendations given in the "Guidelines for officers on protection of personal data" in WG 29 (Guidelines of the WG 29).

6.1. Mandatory appointment of the DPO

Obligation for appointing a DPO have:

- ***all public bodies***[21], except when courts act within their jurisdiction,[22]
- controllers whose ***main activities*** are consist of processing of personal data due to their nature, scope and/or goals requires regular and ***systematic monitoring*** of data subjects ***in great extent*** and
- controllers that deal with special categories of personal data or data relating to criminal convictions or offenses.

The obligation of appointing DPO also applies to the controller and the data processor.

The Regulation does not define what is meant by the ***main activities*** under the ***regular*** and ***systematic monitoring*** of data subjects, nor define what is meant by personal data processing in ***great extent***.

In accordance with the ***Guidelines of WG 29***:

- *as **public bodies** should be consider all private companies with public authority or activities from public interest,*
- as ***main activities*** of the controller are considered key operations necessary to achieve the objectives of the controller, thus main activities cannot be only those dedicated to the controller within the framework of the data that have been processed, but also other activities that will result with processing of personal data, [23]
- ***regular and systematic monitoring*** of data subjects includes all forms of tracking and profiling of the Internet, taking into consideration that the term monitoring is not limited to the online environment, [24]

[20] WG 29 is formed on the basis of Article 29 of Directive 95/46 / EC of the European Parliament and the Council. It is composed of representatives from the supervisory authorities for the protection of personal data of each EU Member State, representatives of the European supervisor for data protection and EC officials. In the frame of their authorities, WG 29 provides advice to Member States on issues related to protection of personal data, provides opinions of EC laws concerning the protection of personal data and on its own initiative provide opinions and recommendations on issues related to protection of individuals in the processing of their personal information within the EU. Since June 2007, the Directorate has observer status in WG29.
[21] Regardless of what kind of data processed and to what extent
[22] Courts are obliged to appoint a DPO who will take care of compliance with the regulations on personal data protection during the processing operations if that is outside of their jurisdiction
[23] Example: Providing services in the field of electronic communications, profiling, tracking location via mobile applications, monitoring fitness and health data through mobile applications and more.
[24] Example: Providing services in the field of electronic communications, profiling, tracking location via mobile applications, monitoring fitness and health data through mobile applications and more.

Project funded by the European Union
Project implemented by Consortium led by Vialto Consulting
Project contacts:
18 Goce Delcev Blvd (14th floor)
1000 Skopje
+389 2 3230 635 ext.116

- ***recommendation of WG 29*** is to assess whether the process personal data ***significantly or not,*** and to take into account the following factors:
  - *number of subjects of personal data,*
  - *the volume of data being processed,*
  - *duration of data processing,*
  - *geographical distribution of the processing,*
- unless it is obvious that a controller has no legal obligation to appoint DPO, ***recommendation of WG 29*** is that each controller should make the internal analysis of the relevant factors and criteria in order to determine whether to appoint DPO or not. Controller who has no legal obligation to appoint DPO, can be done on a voluntary basis. Controller, who appointed DPO voluntary, will have the same obligations as the other controllers that have a legal obligation to appoint DPO.

6.2. DPO- employed or subcontracted with the controller

Regulation establishes that DPO may be:

- ***employee*** of the controller or
- ***sub-contracted by*** the controller based on the contract to provide services.

*In accordance with the **guidelines of the WG 29**, a contract for services may be awarded to an individual or a foreign company. In the second case, it is essential that persons suggested by the company must meet the necessary conditions and must be able to perform the requested duties of DPO, but also to be protected from the possibility of arbitrarily termination of their contract. Also, based on the service contract instead DPO as an individual, whole DPO team can be hired, with the right combination of individual qualifications and personal skills of team members. In any case, the team must have a clear distribution of tasks and be managed by one person.*

6.3. One DPO for more than one controllers

Regulation provides an opportunity to appoint a DPO, in the following cases:

- more companies that work together in a group can appoint one DPO, if he is easily ***available to each of the companies***;[25]
- more public authorities or bodies to designate one DPO, governed by their organizational structure and size[26]

*In accordance with **Guidelines of the WG 29**, the availability of DPO would require its accessibility to data subjects, the supervisory authority (the Directorate), and availability within the controller. The clarification about the availability of DPO when he was appointed in more than one controller, applies to public and private sector.*

[25] In the private sector, two or more smaller companies (with fewer employees or a smaller quantity of operations of data processing) that works together in a particular group, to be able to assign a DPO. Meanwhile, he can be hired on a contract basis to provide services.
[26] In the public sector, two or more public authorities or bodies (with fewer employees or a smaller quantity of processing operations of personal data) that have complex organizational structure, may appoint one DPO. Meanwhile, he can be hired on a contract basis to provide services

Project funded by the European Union
Project implemented by Consortium led by Vialto Consulting
Project contacts:
18 Goce Delcev Blvd (14th floor)
1000 Skopje
+389 2 3230 635 ext.116

6.4. Obligation for publishing the contact data with the DPO

Regulation establishes also obligation of the controller ***to publish contact details for the DPO and to communicate them with the supervisory authority.***

The goal is an easy way to provide direct contact and communication of the DPO with data subjects and the supervisory authority. Following data are considered as contact data: phone number and e-mail address, special contact form on the website of the controller that also can be created. This provision does not provide the name of DPO as part of the contact.

Recommendation of the WG 29 *is the Supervisory Authority (Directorate) to be informed about the name and contact details of the DPO and to be published on the website of the controller, in the internal telephone directory and in the internal organizational scheme.*

6.5. Obligation for secrecy and confidentiality of data

In accordance with the Regulation ***DPO has obligation of secrecy and confidentiality in carrying out its tasks***, but in the same time is not prohibited to contact and seek the advice of the supervisory authority (the Directorate).

Project funded by the European Union

Project implemented by Consortium led by Vialto Consulting
Project contacts:
18 Goce Delcev Blvd (14th floor)
1000 Skopje
+389 2 3230 635 ext.116

7. Which professional standards should be fulfilled by new DPO?

With the new legislation and its implementation it is expected the DPO to gain strategic and independent position in order to achieve more efficient performance of this role and a higher level of personal data protection.

Transposition of the regulation into national law will provide DPO to have professional qualities, expert knowledge of regulations and practice, and the ability to carry out his tasks and will guarantee the obligation of the controller the independence of his position. [27]

This Guide defines all professional standards in details that should be met by the candidate to be appointed as DPO and get a position in the sense of the provisions of the Regulation.

Main goal of this professional standards are:

- identify the profile of skilled and professional person who is appointed as DPO,
- define the minimum standards relating to the position of DPO that should be designed in a way that would ensure its independence.

It is recommended that during the appointing of the DPO controller to monitor the ***professional standards*** presented in the table below:

[27] Article 38 of the Regulation

7.1. DPO profile

Requirements for appointment	***Professional requirements*** ➢ higher education - university degree;[28] ➢ expert knowledge of the regulations and practice in the field of protection of personal data, which involves comprehensive knowledge of these regulations, practice and knowledge of the correlation between these regulations and already established technical infrastructure; *Moreover, because it is not specifically defined:* ➢ *level of expert knowledge, depends on the size of the controller, the complexity and quantity of processing operations of personal data and the sensitivity of personal data;* ➢ *this knowledge to be complemented with adequate knowledge of the organizational structure and controller tasks, and in the public sector with knowledge of the administrative procedures of public authority or body;* ➢ *this knowledge to be complemented with the experience in cooperation with other areas and sectors of the controller, in particular providing advice on issues related to the protection of personal data.* ***Personal qualities*** ➢ personal skills: integrity, initiative, organization, discretion, perseverance, interest and motivation to carry out this function, a high level of professional ethics, skill development and implementation of a particular practice and imposing changes when necessary, and as very important ability to perform tasks to transfer knowledge and demonstrate a clear position, but to affirm himself and his position when needed ➢ Interpersonal skills: communication, negotiation, dismiss-ing conflicts. ***Professional experience*** ➢ 3 years of relevant professional experience.[29]

[28] It is desirable DPO to have a university degree in law or in the field of information technologies, but this is not a limiting factor and person with a university degree in another area can be appointed to this position.
[29] Relevant experience means experience in the implementation of regulations on protection of personal data, as well as knowledge of the organizational structure and operation of the controller. If the required experience is missing, the controller should enable the DPO to get the necessary training in this area

Certification of the DPO, maintenance and upgrading of expert knowledge	***Legal requirement for certification*** ➢ issuing a certificate* of completed training for DPO as proof of the expert knowledge of the regulations and practice in this area and as a requirement for appointment of the DPO. ***Legal obligation to maintain and update expert knowledge*** After the appointment to this job position: ➢ monitoring of regular trainings organized by the Directorate, as well as certified training courses organized by external service providers that have accreditation for providing this type of service (professional organizations) - domestic or from a EU member state; ➢ introducing new forms of trainings as a mean of self-improvement through the network of officers.[30]

[30] See point 9.3

7.2. Position and status of DPO

Expertise and skills	The fact that DPO is a part of the controller gives an ideal opportunity to ensure compliance with the regulations on protection of personal data from the inside, providing appropriate advice or intervening when necessary to avoid possible actions by the Directorate. But, although DPO is part of the controller (employed or subcontracted with the controller), governed by the nature of his job position, he will be independent within the controller. The new legal solution will be designed in a way that ensures independence of the DPO or performance of the function without any influence and instructions. But DPO independence does not mean that he has the authority to make decisions. That would mean overstepping his powers. The controller is responsible for ensuring compliance with the regulations on protection of personal data and to demonstrate compliance with these regulations, and DPO should be a key figure through which the controller will fulfil this obligation. If the controller made a decision that is incompatible with the rules and advice given by DPO, DPO be able to provide separate opinion.
Guaranteeing the independence	independence of the DPO function, the controller will ensure setting up the rules: ***Involvement of the DPO in all matters related to the protection of personal data*** ➢ DPO should be appropriately and in timely manner (early stage) included in all issues related to protection of personal data. ***Appointment and dismissal*** ➢ Appointment for an indefinite period of time or for as long as possible period of time; ➢ Registration of the appointment of officers of the Directorate ➢ Dismissal / revocation from office only if DPO no longer meets the requirements for performing tasks.[31] ***Human and other resources*** ➢ Providing the necessary human and other resources to carry out the tasks for providing access to personal data processing

[31] Additional protection of the job position of the DPO can be achieved with the prior consent of the Directorate for cancellation / dismissal of the DPO.

	operations of data, especially for maintenance and upgrading of expert knowledge; ➢ Develop a work plan to assess the need for human and other resources; ➢ Active support by the highest level of leadership / management in terms of providing staff, financial resources and infrastructure suitable for the DPO job position ***Exemption from other duties*** ➢ Appropriate exemption from other duties to DPO in order to be focused on the tasks arising from this function. ***Conflict of interest*** ➢ If DPO performs other tasks, guarantee should be provided that no conflict of interest between the duties arising from his office and other official duties.[32] To prevent a conflict of interest as a good practice the controller should consider the following: ➢ to identify positions that are incompatible with the tasks of the DPO; ➢ to design internal rules to prevent conflicts of interest; ➢ controller pleaded that DPO does not have conflict of interest as a way of raising awareness about the issue ***Setting the controller*** ➢ In the organizational structure, DPO will manage the organizational unit for the protection of personal data (if established) or will manage the office as a person that is appointed to appropriate hierarchical level [33] that would guarantee its independence in acting, i.e. his position to be managed in a manner that will prevent any impact or receive instructions when performing tasks ➢ Exclude the possibility of being dismissed or penalized for carrying out its duties;[34] ➢ Regulation of the cooperation with the highest level of management / management's internal regulations;

[32] Because of the diversity of the organizational structure and placement of each controller, the existence or non-existence of conflict of interest should consider each case
Example: DPO cannot be placed simultaneously in a position to determine the purposes and means of processing personal data

[33] It is recommended the DPO to be placed in a supervisory / management position

[34] DPO may legitimately be dismissed from office for other reasons, but not for the performance of his duties

	➢ Informing the highest level of governance / management on important issues in this area, at least on a quarterly basis and holding thematic meetings, whenever necessary; ➢ Directly responding to the highest level of management; ➢ visibility of the function in the organizational structure; ➢ Regulation of the obligation of all employees to cooperate with DPO without waiting for prior permission from his supervisor; ➢ Adopt internal regulations that govern the cases in which consultation is mandatory DPO; ➢ Authorising the DPO for signing of correspondence concerning the protection of personal data; ➢ The appointment of deputy DPO in order to ensure continuity in the role in the absence of DPO. For the Deputy DPO should be provided the same guarantees for carrying out their functions in an independent manner.[35] ***Regulations for implementation revisions/controls/ checks*** ➢ Following the authorization of DPO for conducting audits / controls / checks[36], the controller should adopt detailed rules for regulation. DPO have access to the premises and systems where they perform operations on data processing, and an obligation to communicate with persons who have addressed for violation of legislation in this area.

[35] This is especially recommended for larger controllers or controllers with a large quantity of processing operations of personal data
[36] Article 39, item 1 b of the Regulation

Elements which weaken the position of DPO	➢ If DPO performs other tasks except the tasks arising from his office, he continuously faced with a conflict between time dedicated to the tasks that are not directly related to the function of DPO and intention to complete the tasks arising from this job position. Thus if superiors gives more weight to other tasks, it creates pressure to the DPO to concentrate on those tasks. This can lead to inefficient performance of tasks arising from the job position of the DPO. Furthermore, it is likely be in a conflict of interest between the tasks to fulfil as DPO and other tasks. ➢ If DPO has a fixed-term contract, he is more unfavourable position and probably less persistent and tenacious in performing tasks compared to DPO who has a contract of indefinite duration. The concern stems from whether it will be renewed agreement or not. ➢ It is likely that DPO responsible to or is controlled by their direct supervisor, may feel pressure and its independent conduct in performing the function may adversely affect the development of his career. The correct and proper execution of the tasks of the DPO very often implies that he should take a firm stand that often can be in contrast to his superiors and to demand fulfilment of obligations by persons who hold high positions in the controller due to that the DPO often is perceived as a "bureaucrat" or "troublemaker." It is very important DPO to have autonomous status which will help him to withstand the pressures and difficulties that go along with this important function. That is why, to alleviate pressure the DPO should fit and be controlled directly from the highest level of management / cross-managed by the controller. ➢ DPO who is in a position to require human and other resources from their direct supervisor, may face difficulties if the direct supervisor is not fully committed to achieving compliance with the regulations on protection of personal data. This will avoid if DPO has its own budget and if his requests are subject to approval by the highest level of governance / management of the controller

7.3. Recommendations for controllers with different size

Criteria for categorization	It is difficult to establish the criteria based on which controllers would be deployed in different categories, depending on their size, because there are controllers with a small number of employees, and a large quantity of processing operations of personal data or sensitive personal data, or conversely, controllers with many employees who do not perform other processing operations of data, other than data processing to its employees. Hence, it is difficult to determine fewer obligations during performance of DPOs tasks in smaller compared with the performance of these tasks in larger controllers. On the other hand, it is a fact that small controllers do not have sufficient human and financial resources to meet the legal obligations related to the performance of this function. Therefore, future legislative solution will contain provisions that will allow small controllers or controllers that have a small quantity of processing operations of personal data to fulfil the legal obligation.
Small controllers	➢ A DPO to be appointed for more small controllers that will work together in a certain group or controllers that do not have complex organizational structure.[37] ➢ DPO can be hired on a contract basis for providing services. ➢ If DPO performs other tasks, to provide assurance that there is no conflict of interest.
Large controllers	➢ To appoint a DPO on a full-time position, which is established to perform his tasks. This would mean appropriate excuse from the other responsibilities in order to be able to perform the tasks arising from the job position. ➢ To provide the necessary human and other resources in order DPOs tasks to be fulfilled. If the workload requires, a team, led by the DPO, should perform DPOs tasks. The internal structure of the team, as well as duties and

37
The new legal solution to provide the opportunity to be appointed an officer for two or more small controllers (controllers with few employees or a small quantity of processing operations of personal data). He can be hired on a contract basis to provide services.
In the public sector in this way to treat public bodies or bodies which have a complex organizational structure.
In the private sector in this way to treat related companies that operate in a particular group.

	responsibilities of each team member must be clearly defined. ➢ Controller to introduce the "Data Protection Impact Assessment"[38] - impact assessment of the planned operations of data processing on the protection of personal data, if such a process is not yet established.

This Guide offers several forms[39] that will contribute in performing of the DPO tasks:

- Legal act that will regulate the determination/appointment of the DPO;
- Job description of DPO as integral part of the employment contract, which can serve as an example of the controllers that with act of systematisation need to foresee particular job position for the DPO or with the act for internal organization foreseen organizational unit for the protection of personal data;
- Reporting to the Directorate for defining/ appointing of DPO;
- List of self-evaluation filling on an annual base, DPO will check whether it is in accordance with the regulations on protection of personal data, monitor its progress in meeting commitments and, if necessary, be adjusted;
- Analyse of the workload of the DPO that would lead to conclusion whether the workload can be fulfilled during working hours or to perform the duties is necessary for additional human resources, or whether the workload allows performing other tasks unrelated to this function during working hours;
- Minutes of the meeting held between DPO and organizational unit of the controller;
- Checklist for handover of duties from the old to the new DPO, which can be used in the handover of tasks from DPO to his deputy.

[38] In this Guide English term for the process is used, because the process is well known as „Data Protection Impact Assessment“

[39] See Annex to the MAIN part, Template 1, 2, 3, 4, 5, 6 и 7

8. What will be the tasks of the new DPO?

Current tasks performed by the DPO are in accordance with the applicable LPDP and will have to be adapt to the tasks set out in the Regulation[40]***. This handbook elaborates in detail the tasks of the DPO stipulated in the Regulation, which will accordingly be translated into new legal solution.***

8.1. Informing

DPO will be obliged ***to inform*** data subjects about their rights, but also to inform the controller of his obligations under the regulations on protection of personal data.

Also, DPO will take care to fulfil the rights of data subjects and the obligations of the controller. These rights and obligations are thoroughly described in the SPECIAL CHAPTER of this Guide

8.2. Monitoring of the compliance with the regulation

DPO is obliged to ***monitor compliance*** with the regulations on protection of personal data and to ***ensure internal compliance*** with these regulations controller[41]. Specifically, the controller DPO helps in ensuring internal compliance with these regulations. DPO collect information to identify the operations of the data processing, analysis and verification of compliance with regulations; and provide information, advice and recommendations to the controller.

DPO is not personally responsible in case of non-compliance with the regulations on protection of personal data. Compliance with these regulations is the responsibility of the controller.

The Regulation makes clear that the controller will ensure compliance with its provisions and shall demonstrate that the data processing is performed in accordance therewith, the DPO is a key figure through which the controller will fulfil this obligation.

Compliance and monitoring of the compliance with the regulations on protection of personal data, in particular means: respecting the principles of protection of personal data and the processing of data by the controller, preparation of documentation for technical and organizational security measures and privacy when processing personal data and its implementation, reporting on collection of personal data and respect the rules of video surveillance. With the new legal solution, the controller will have an obligation for notification of security breaches of personal data. [42]

8.3. Raising of the awareness

Raising awareness of employees of the controller for the right to protection of personal data ***will be one of the key commitments of DPO*** that affirm this right of the individual and educate the controller of his obligations arising from the regulations on protection of personal data.

[40] Article 39 from the Regulation
[41] This obligation is similarly provided with current LPDP
[42] See the Special part of the Guide

Project funded by the European Union
Project implemented by Consortium led by Vialto Consulting
Project contacts:
18 Goce Delcev Blvd (14th floor)
1000 Skopje
+389 2 3230 635 ext.116

DPO should work on finding as many activities as possible that will act to raise employee awareness of the controller, especially those involved in processing operations of personal data.

8.4. Training for the employees

Current LPDP prescribes the obligation of the DPO to offer[43] training to employees regarding the protection of personal data. Regulation advocates that one of the tasks of the DPO is conducting training of staff involved in the operation of data processing. ***The explicit obligation to perform training by the DPO*** respectively will be transposed into a new legal solution.

In this Guide a form[44] is proposed - Register of training, through which the controller has a record of employees who participated in trainings with details of the type and the topics covered by training.

8.5. Providing advices and recommendations to the controller

DPO will be obliged to ***advise the controller to fulfil the obligations*** arising from the regulations on protection of personal data and ***recommendations for practical improving*** of the protection of personal data.

Advice can be given verbally or in writing. If the advice given for a particular case, can be applied in other similar cases, it is recommended to be published on the website of the controller. In case when the DPO is in dilemma what kind of advice should be provided to the controller, it is recommended to consult the supervisory authority (the Directorate).

DPO gives recommendations to the controller for practical improvement of data protection. These recommendations can be given on its own initiative or at the request of the controller.

8.6. Performing audits / controls / checks

DPO will be authorized (alone or with appropriate support) to ***carry out audit/control/verification of compliance***[45] with the regulations on protection of personal data controller. For this purpose, the controller should provide all relevant information and documents, and to provide access of the DPO to all data as requested.

The procedure and the way on which the DPO will perform audits / controls / checks should be regulated by an internal act of the controller.

In this handbook several templates[46] are proposed that can be used in carrying out audits / controls / checks:

- Annual plan for their implementation;
- Checklist for determination whether all preparatory activities are set out for their implementation;
- Report on conducted audit / control / inspection with catalogue of proposed corrective measures and recommendations;

[43] The nomination of training does not imply that the DPO has an obligation to apply them
[44] See Annex to the main part: form 8
[45] Controller to decide which term to use for this procedure
[46] See Annex to the main part: form 9,10,11,12 and 13

Project funded by the European Union
Project implemented by Consortium led by Vialto Consulting
Project contacts:
18 Goce Delcev Blvd (14th floor)
1000 Skopje
+389 2 3230 635 ext.116

- Table for following the findings of audits / controls / checks carried out in the controller by DPO or another organizational unit, and inspection of the Directorate and external controls;
- Registry for recording all conducted audits / controls / check / inspections.

8.7. „Data Protection Impact Assessment“[47]

The introduction of a tool for assessing the impact of the planned operations of data processing on the protection of personal data "Data Protection Impact Assessment" is the most effective way of complying with the regulations on protection of personal data and to meet the expectation of the subjects to respect their privacy.

Although the implementation of the "Data Protection Impact Assessment" is the task of the controller, however ***DPO has an important and useful role by providing specific advice and monitoring whether the advice given and accepted*** are respected by the controller. If the controller does not accept the advice given by OZLP, the documentation should adequately state the reasons or justification for their rejection.

This tool allows the controller to identify and resolve problems early in the development of new systems and new products and to reduce unnecessary costs and potential reputation damage as possible side effects.

This tool is already established in some controllers in the private sector, especially in banking and electronic communications.

8.8. Cooperation with the Directorate and acting as a contact point for the Directorate

DPO in the public and private sectors have established cooperation with the Directorate which consists of giving support by the Directorate on matters related to the execution of their office, information sharing and other communications. Its cooperation with the Directorate allows OZLP easier to ensure compliance with regulations in this area. They participate in training organized by the Directorate and they are considered not only as a form of deepening and upgrading of expert knowledge, but also as another form through which reinforces cooperation with the Directorate, and the cooperation between DPO.

The strengthening of cooperation between the Directorate and the controllers is ***essential to establish higher standards*** of respecting the right to protection of personal data. The ***DPO has a crucial role*** to strengthen this cooperation.

DPO acts as a contact point, which facilitates communication between the Directorate and the controller.

8.9. Risk-based approach

DPO regulation provides that, in carrying out tasks should take into account the risks associated with processing operations, and the nature, scope and purpose of processing personal data. This means that ***DPOP will prioritize*** and focus ***on issues that present a higher risk*** for the protection of personal data. Based on its pragmatic approach, OZLP will

[47] The title is written in English, because this process (impact assessment of the planned processing operations of personal data on the protection of personal data) is everywhere known English expression

determine which areas to be subject to internal or external audit / control / verification, such training to be organized for employees and that employees, of which operations of data processing to pay more attention

Project funded by the European Union

Project implemented by Consortium led by Vialto Consulting
Project contacts:
18 Goce Delcev Blvd (14th floor)
1000 Skopje
+389 2 3230 635 ext.116

9. Tools to strengthen the job position of the DPO

In order to strengthen and to make it more efficient the work of the DPO and in order to intensify the cooperation with the Directorate and to establish new forms of cooperation between DPO, it is proposed preparation of the new tools, including:

9.1. This Guide

This Guide is a tool that serves to ***carry out the tasks of the DPO in efficient way***, helping the DPO to inform about the news that we introduce into national legislation, and in particular to better understand their function, and become aware of the new position of the controller, but also helping controllers to learn and to implement obligations under the Regulation.

9.2. DPO corner (DPO Corner)

So far, cooperation with the Directorate is aimed at advising the controllers to improve their current operations and to the development the best practices on specific topics. In order to intensify this cooperation, the existing website of the Directorate ***will establish Officers Corner (DPO Corner) as a new form of cooperation***. Access to the Corner of officers will be restricted only to the Directorate and for DPOs.

Efficient DPO can only be one that is well informed about the regulations on protection of personal data and on current progress in this area. Corner of officers will serve as a platform for exchange the knowledge and experience and support in performing their tasks.

DPO will have access to updated documents that are focused on their role and tasks. The documents will be designed in a way that will allow you to get a clear idea of this feature.

The DPO will have access to tools for providing support in the performance of their duties. This indicates forms, and presentations that will help to strengthen the public awareness of employees of the controller or processor where DPO is appointed.

Corner of officers will include a section devoted to current events (conferences, seminars, trainings and meetings) that can be attended by DPOs for improving their knowledge and skills or to secure the necessary tools to perform their tasks.

9.3. Network of DPOs

In order to implement the cooperation and exchange of experience among DPOs, network of officers will be created. Considering the importance of interaction with their colleagues, especially considering how important the sharing of best practices and know how is, this Network will be a useful tool for better information and more efficient functioning of DPO.

The network of officers will be created as a separate section within the DPO Corner, where DPOs will be able to identify their colleagues. The network should be designed in a way that will allow easy establishment of cooperation in general, but also at sectorial level. This network of officers should prove as useful in producing advices and exchange of views on common issues and problems.

Project funded by the European Union

Project implemented by Consortium led by Vialto Consulting
Project contacts:
18 Goce Delcev Blvd (14th floor)
1000 Skopje
+389 2 3230 635 ext.116

Within the network of officers, it is desirable to form separate groups at the sector level of cooperation and exchange of experience.

9.4. E-forums (e-conferencing)

Creating an online web tool for organizing e-forums (e-conferencing) to allow ***communication between DPOs,*** harnessing the benefits of the modern web.

Through this tool, DPO will have the opportunity to be timely informed about the novelties in the field of protection of personal data and will also exercise ongoing communication. The e-forum will create new topics on current issues, DPOs will have the opportunity to exchange views and experiences in relation to each particular topic. E-forum will enable video communication in one direction, from the Directorate to DPOs with the opportunity to submit questions by DPOs in real time.

It is desirable to initiate e-forums (e-conferencing) and sectorial level.

9.5. Association Officers

As an additional form of cooperation between DPOs ***may be based Association officers***, on their own initiative.

9.6. New curriculum for training

As support to the implementation of the new law (after its adoption) which will strengthen the job position of the DPOs ***will develop a new training curriculum and will prepare new materials for learning and training,*** to be used by members of the Commission for training in the Directorate. In the training materials practical steps that need to be taken will be defined in order to meet the obligations that will arise from the new legal solution. They will be printed, but also published in electronic form.

It is desirable to have organisation of trainings at the sectoral level which will help to implement the new LPDP.

9.7. Communication strategy

Communication Strategy is a valuable tool that will support the implementation of the new legal decision after transposition of the Regulation. ***One part of the communication strategy will be devoted to the new role of the DPO.*** Communication Strategy will provide for organizing public events and to raise awareness and promote the job position of the DPOs.

9.8. „Days of awareness“

It is recommended to organize "Days of awareness" as another tool to promote new role of the DPO. ***On this event "Days of awareness" the heads of public bodies and the managers of private companies should be invited*** in order to introduce them to the profile, position and tasks of the DPO and the conditions and circumstances in which he/she will performs his/her tasks. It is also recommended to establish a practice of regularly organizing "Days of awareness“.

Project funded by the European Union
Project implemented by Consortium led by Vialto Consulting
Project contacts:
18 Goce Delcev Blvd (14th floor)
1000 Skopje
+389 2 3230 635 ext.116

SPECIAL PART

The specific part of the Guide ***elaborates the rights of data subjects and the obligations of the controller*** arising from the regulations on protection of personal data, as well as ***activities undertaken by the DPO*** for effective exercise of rights of subjects and fulfilling the obligations of the controller.

10. Rights and obligations

The specificity of regulations on protection of personal data is consist from the fact that for the data subjects are planned rights, exclusively, and for the controller obligations, exclusively.

10.1. Right of the data subjects

- ***To be informed about the processing of their personal data***

Related to the transparency, the controller is obliged to inform data subjects about the purpose and legal basis for the processing of their personal data.

- ***To request access to data***

Request for data access must be submitted in writing and contain additional data and information necessary to locate the requested information.

Within 15 days of receipt of the request, the controller has an obligation to provide respond to the subjects, with no obligation to respond again at the same or similar request to a specific entity, if in the meantime there is no changes in his personal data, unless there is a six month period from the date of submission of the previous until the submission of the new request.

- ***To require amendment, modification, deletion or suspension of data processing***

At the request of the subjects, the controller is obliged to supplement, amend, and delete personal data or to stop data processing, if they are incomplete, inaccurate or out of date or if their processing is not in accordance with law.

Regardless if the entity has submitted such a request, if the controller determines that the personal data are incomplete, inaccurate or out of date, he is obliged to supplement, amend or delete.

The controller is obliged within 30 days of receipt of the request, to notify the entity for new amendments, alterations or deletions.[48]

An integral part of this work is the form[49] - Request for access and correction of personal data.

[48] In order to achieve balance between the right to privacy and the importance of national or public interest or social need can restrict the rights of subjects of personal data. LPDP stipulates that these rights can be limited due to: the protection of the security and defence of the country; detection and prosecution of offenders; protection from violation of ethical rules of a particular profession; protection of important economic or financial interests of the state and protect the rights and liberties of the subject or the rights of other individuals.

[49] See Annex to the specific part: Form 14

10.2. Obligation of the controller

10.2.1. Respect of the principles of protection of personal data

The controller is obliged to act in accordance with the principles of protection of personal data:

- ***Legality, fairness and transparency***

To assess whether the processing of personal data is ***fair***, of particular relevance is the ***transparency*** or informing the data subjects on the processing of their data. Entities should be informed of the purposes for which they collect and process their personal data. Processing of personal data ***in accordance with Law*** means any legal basis and respect the legal constraints originating from other laws.[50]

- ***Limitation of the goals***

Personal data are collected ***for concrete, clear and legally determined purposes*** and shall not be processed in a manner that is consistent with those goals. The data can also be used for purposes other than those lawfully collected only if there is a legal basis for data processing and other purposes.[51]

- ***Minimize the data for processing***

The data must be ***adequate, relevant and not to a greater extent*** than is necessary to fulfil the purpose for which it was collected. "Principle of necessity" limits the scope of data that can be processed, only to those that are necessary to fulfil the purposes for which they are processed.[52]

- ***Accuracy***

This principle applies to data quality. They should be accurate and where necessary updated. The controller takes care of the ***accuracy*** of the data and is obliged to ***update*** or supplement, when necessary.[53]

- ***Limitation of data keeping***

The data ***should be kept*** in a form which allows identification of the personal data subjects ***no longer than is necessary to achieve the objectives***. This principle limits the period in which data can be lawfully processed, and after termination of the purposes for which they were collected, should be deleted or destroyed, or to be anonymized. When the controller for

[50] Example: The Law on Electronic Communications stipulates that operators are obliged to keep records of all subscribed customers, which shall contain the following data: name, surname, address and identification number. The processing of these data by the operators are carried out according to law.
[51] Example: Personal data of the employee are processed by the employer in order to realize the rights and fulfillment of obligations and responsibilities arising from the employment contract. If the legislator with specific legal decision impose on the employer's obligation names of employees to bring in another collection of personal data for the exercise of certain rights of employees who do not stem from the employment contract, the employer performs data processing for the purpose other than the original for They were collected
[52]Example: If a person fill the Application form in order to participate in the lottery, it is sufficient to state their name and contact information (home address or phone number). The data on the marital status or the personal identification number is irrelevant, inappropriate and excessive in relation to the objective to be achieved. If the employer requires the candidate applying for employment to submit a photograph, this personal data is irrelevant, inappropriate and too large in relation to the objective to be achieved. Regardless of the type of business relationship established, the processing of data about nationality by banks for their customers, or by operators of electronic communications services to their customers would be irrelevant, inappropriate and excessive demand.
[53] Example: Office for Civil Registration as a body within the Ministry of Justice who runs the record keeping in accordance with the Civil Registration is required to continually update it, ie the replacement of the existing data of citizens with new (change the name, address and so on.)

Project funded by the European Union
Project implemented by Consortium led by Vialto Consulting
Project contacts:
18 Goce Delcev Blvd (14th floor)
1000 Skopje
+389 2 3230 635 ext.116

a particular category of personal information will determine the terms of their storage shall be deemed that the acts is in accordance with this principle.

Typically, these rules are being implemented through the introduction of appropriate procedures in accordance with regulations on archive and office work.[54]

- ***Integrity and confidentiality***

Regulation prescribes the principle of integrity and confidentiality, according to which data should be processed in a manner ***which ensures an adequate level of security of personal data,*** including protection against unauthorized and unlawful processing and protection from accidental loss, destruction or damage by applying appropriate technical and organizational measures.

- ***Request for accountability***

Regulation introduces a new ***requirement for accountability***, according to which the controller is responsible for compliance of its operations with these principles and should be able to demonstrate compliance with these principles.

10.2.2. Legitimacy of the processing of personal data

The controller has an obligation to make the personal data processing legitimate. Processing of personal data is done if there is:

- ***Legal obligation***

Typically the legal basis for processing personal data are located in the legislation of a particular sector or area.[55]

- ***The consent of the data subject***

The controller has an obligation to prove that the subject has given consent to the processing of his personal data. If consent is given in a written form should be presented in an understandable and easily accessible form, using clear and simple language. The entity has the right to withdraw consent at any time. The withdrawal of consent does not affect the lawfulness of the processing based on consent before its withdrawal.

To assess if the consent to the processing of personal data is voluntarily given by the entity (subject) first should be determine if the rights and obligations of the agreement is conditional on the given consent.[56]

The processing will be considered legal if it is done in order to:

- ***Meeting the where the subject is a contracted party***

In each case it will be assessed which data are necessary for the objective that need to be achieved by the establishment of a contractual relationship. Moreover, there is no general rule

[54] Example: After the expiry of the insurance contract between the insurance company and the customer, and after expiry of the deadlines for storage according to the regulations for office and filing, documentation with respect to that business relationship should be destroyed.
[55] Example: The Electoral Code is the legal basis for processing personal data of citizens in the voters list.
[56] Example: The operators of electronic communications services, banks, insurance companies or any other companies, after establishing business relationship with users, customers, insurers can use their personal data for performing direct marketing solely based on their explicit consent which should be in a form that allows them to state whether the data can be used for this purpose or not. Based on this agreement, it can be performed processing of their personal data only for direct marketing purposes, but not for other purposes

upon which selected data that would be considered as necessary for a particular goal, so each specific contract should be thoroughly reviewed.[57]

- ***Meeting the legal obligation of the controller***

Each controller has an obligation to disclose personal data from their collections, when there is a legal basis.[58]

- ***Protection of life or vital interests of the entity***

This means that the processing of personal data can also be done to protect the physical and moral integrity or other vital interests of the data subject.[59]

- ***Execution of works of public interest or of official authorization***

The reference to this legal basis, sometimes is a risk of discretionary treatment. To prevent this, following criteria should be taken into consideration:

In the public sector, execution of works of public interest or performance of official authorization of the controller or the third party to whom the data are disclosed, must have a base in the law. In the private sector, the authorization must have a basis in a certain legal act.[60]

- ***Meeting the legitimate interest of the controller***

Every interest that is not contrary to fundamental legal principles, can be considered as legitimate, but if the data processing would jeopardize fundamental rights and freedoms of the data subject, the prevailing interests and the processing will not be allowed. Hence, the balance of interests can serve as a legal basis for the processing operations of personal data that cannot come under any other legal grounds.[61]

10.2.3. Technical and organizational measures for secrecy and data protection

In order to fulfil the obligation arising from LPDP and Rulebook on technical and organizational measures to ensure confidentiality and protection of personal data of the Directorate, the controller ***adopts documentation and undertake technical and organizational measures*** to ensure the security and confidentiality of the processing of personal data that will prevent unauthorized access, change the data, their unauthorized disclosure, accidental loss or

[57] Example: In general, in any contract is subject of the processing of personal data of natural persons or representatives of legal entities as parties (name, place of residence, identification number, identity card), but what about other personal information be processed depends on the object of the contract and the purpose for which the contract

[58] Example: The natural and legal person, the state authorities or other bodies are obliged to submit personal information to the competent courts for their performance as evidence in litigation, when these data are requested in the manner prescribed by law.

[59] Example: In exceptional cases, such as natural disasters, emergency or martial law, etc., the competent authorities shall have the right to disclose certain personal data (name, location) to be able to find or save a person.

[60] Example: The Institute for Public Health and the Centres for Public Health in order to perform work in the public interest - the timely prevention of the spread of infectious disease, carry out processing of personal data of infected persons, and persons which were in contact with the infected

[61] Example: Personal data on a specific subject (name and phone number) are publicly published telephone directory for a specific purpose - achieving contact. These personal data previously published in a telephone directory – contact person, also they can be processed for another purpose - conducting research if the subject is asked whether he agrees to participate in the survey. Meanwhile, such processing of personal data will be seen as legitimate, especially if it endanger the freedoms and rights of the subject. But using data from the phone book to perform direct marketing cannot be subsumed under this legal basis, because in LPDP expressly stated that direct marketing can be made solely on the explicit consent of the data subject.

Project funded by the European Union
Project implemented by Consortium led by Vialto Consulting
Project contacts:
18 Goce Delcev Blvd (14th floor)
1000 Skopje
+389 2 3230 635 ext.116

destruction. One of the primary tasks of DPO to monitor compliance of the controller with this documentation. [62]

This handbook offers several useful forms[63] the documentation of technical and organizational measures:

- Statement to ensure confidentiality and protection of personal data;
- Authorization to perform processing of personal data;
- Registration of persons authorized to perform the processing of personal data;
- Records for personal data provided to the user;
- Register of risks.

10.2.4. Notification of the personal data collections

The controller before starting the processing of personal data is ***required to report the collection of personal data*** in the Central Register of collections in the personal data of the Directorate. [64]

Central Registry enables practical application of one of the rights of the data subject - the right to be informed of the processing operations of personal data. In that way collection of personal information collected by the controller, the categories and volume of data processed become transparent.

10.2.5. Compliance with the rules for video surveillance

Setting the video surveillance at the premises of the controller ***creates an obligation to inform*** the data subjects for space that is under surveillance and recorded.

The notice should be ***clear, visible and publicly stated*** (e.g. at the entrance of the office building). The notice should indicate who is the controller of personal data which are processed with the video surveillance, as well as to be referred in a way in order to receive information where and how long are kept the recordings of the video surveillance system.

Video cameras ***cover only the space*** that is sufficient to fulfil the objectives that are set. Video records can be stored no longer than 30 days, and after expiry of this deadline, the photos must be deleted. Video records can be stored longer than 30 days, only if that is provided with other special legal provisions

[62] The documentation contains: Plan to create a system of technical and organizational measures to ensure confidentiality and protection of personal data; Rules on technical and organizational measures to ensure confidentiality and protection of personal data; Procedure for determining the obligations and responsibilities of the administrator of the information system, authorized persons to access to the documents and information and communication equipment; Procedure for reporting, response and recovery incidents; Procedure for the way for easy backup, archiving and storage, as well as reinstatement of stored personal data; Procedure for the manner of destruction of documents and the manner of destruction, wiping and cleaning of the media; Guidelines for keeping records for authorized persons performing the processing of personal data and transmit media away from business premises controller

[63] Annex to the Special section: Model 15, 16, 17, 18 and 19

[64] Central Registry is available on the website www.dzlp.mk. It is available to controllers to be able to register their collections online through a simple procedure and free of charge

Project funded by the European Union
Project implemented by Consortium led by Vialto Consulting
Project contacts:
18 Goce Delcev Blvd (14th floor)
1000 Skopje
+389 2 3230 635 ext.116

Introducing video surveillance of the controller creates an obligation to enact a special act - Rulebook on video surveillance, which will regulate the place where video cameras will be placed, the space that is going to be recorded, purpose and legal basis for their setting and the person who will perform the control of the system. [65]

Purposes for which video surveillance can be performed are defined in LPDP, and they are:

- protection of life or health of the people,
- protection of life and health of employees due to the nature of their work
- protection of the property and
- control over access to official or business premises.

10.3. New obligation - Notice of violation of personal data

Regulation introduces a ***new obligation***[66] for the controller in the event of a breach or violation of personal data, [67] ***to inform*** the supervisory authority and the affected data subject.

With the transposition of the Regulation in the new legal solution, the ***controller will be obliged to inform the Directorate*** for security violation / infringement of personal data only if that violation / infringement poses is a risk to the rights and freedoms of individuals. Moreover, for any particular violation/infringement the controller will assess whether there is an obligation to inform the Directorate or not [68]

In case there is likely security violation / infringement of personal data to cause high risk for the rights and freedoms of the individual, ***the controller will directly inform the data subject*** [69]

The notification to the Directorate shall contain the following ***information:***

- description of the nature of the violation / infringement and if possible categories and approximate number of affected subjects and categories and approximate number of affected records of personal data;

[65] The content and form of the act to be adopted by the controller is laid down in the Regulation on the content and form of the Act for the manner of conducting surveillance of the Directorate.
[66] Basis to introduce this obligation in the Regulation is Article 4, paragraph 2 of the Directive on privacy and electronic communications 2002/58 / EK, known as „E-Privacy Directive"
[67]As a security breach / violation of personal data shall be considered: physical, material or immaterial harm to the data subject, such as the loss of control over their personal data, restrict the rights, discrimination, identity theft, fraud false identity, financial losses, breaches of confidentiality of personal data or any other significant adverse economic or social consequences for the affected entity
[68] Example: The controller shall inform the Directorate of losing user data, because it could lead to identity theft, but fails to notify the Directorate for loss of data to the list of telephones of employees, because the disorder may not affect the rights and freedoms of individuals
[69] The controller shall have no obligation to inform the data subject of the disorder / injury, if one of the following conditions:
- controller took the appropriate technical and organizational protection measures, including in relation to personal data affected by the violation/infringement;
- controller took the consistent measures to ensure that there is no more likely to have a high risk of freedoms and rights of the entity;
- notification would involve a disproportionate effort, because it is made public reporting or otherwise required to inform the subject.

If the controller failed to notify the entity and the Directorate it will be considered that particular disorder / injury is a high risk of his rights and freedoms, the Directorate may request the controller:
- inform the subject thereof or
- to declare that it has met one of the conditions in which there is no reporting obligation.

Project funded by the European Union
Project implemented by Consortium led by Vialto Consulting
Project contacts:
18 Goce Delcev Blvd (14th floor)
1000 Skopje
+389 2 3230 635 ext.116

- name and contact details of DPO or another contact person when more information should be provided;
- description of possible consequences;
- description of the measures proposed or taken by the controller to deal with the violation / infringement or to reduce the negative effects.

The content of the notice to the data subject will be the same, but the nature of the violation / infringement should be described in simpler language.

The notification shall be made ***as follows***:

Without undue delay and, where feasible, not later than 72 hours after the controller became aware of the violation / infringement. Where the notice is submitted within more than 72 hours to the same should be submitted reasons for the delay.

Obligation for ***documentation*** recording:

The controller shall be obliged to document every security breakdown or infringement of personal data, including the facts related to the violation / infringement, consequences and actions taken to deal with this. The documentation will enable the Directorate to check compliance with this Article.

An integral part of this Guide are the templates[70] - Notification to the Directorate and Notification to data subjects. The templates can be applied after the notification for security violation / infringement of personal data shall be prescribed by the new LPDP.

This obligation is already provided in the Law on Electronic Communications[71] for the Controllers in the field of electronic communications.

[70] See Annex to the specific part: Form 20 and 20a
[71] Article 167 of the Law on Electronic Communications

11. Actions of the DPO

Bellow there is a list of actions that DPO undertaken so as to inform data subjects about their rights, and more effective fulfilment of the obligations of the controller.[72]

11.1. To inform the subjects about their rights

- Publication of useful information and documents (Guides, guides, instructions and guidelines for the protection of personal data) intended for data subjects on the website of the controller;
- Preparation of brochures and leaflets.

11.2. To fulfil the obligations of the controller

- Preparation of internal regulations on protection of personal data, intended for employees that perform processing operations of personal data, especially the controllers with a larger quantity of processing operations of personal data and a number of persons that process personal data;
- Creating a separate section of the corporate website of the controller, designed for privacy and protection of personal data, where all internal regulations on protection of personal data, manuals, guides, periodical reports on the DPO and other documents that may be useful for controller will be published;
- Organize and conduct trainings for the employees of the controller involved in the operation of data processing, based on previously prepared plan for training (on a regular base in a certain time interval);
- Organizing meetings with the highest level of management / management;
- Indication of the obligation to sign the statements on privacy and protection of personal data, issuing authorizations for employees performing the processing of personal data and keeping records of such persons;
- Indication of the obligation to perform external and internal checks, as well as periodical controls on information systems and information infrastructure of the controller
- Preparation of periodic and annual reports on the activities of the DPO.

11.3. Raising awareness of the controller

- Press for the staff;
- Publishing short articles in the existing publications of the controller;
- Issuing information leaflets;
- Publishing content on the website of the controller;
- Organizing activities to celebrate January 28 - European Day for the Protection of Personal Data (brochures, leaflets, quizzes).

[72] The rights of data subjects and the obligations of the controller are elaborated in detail in section 10 of this Guide

Project funded by the European Union
Project implemented by Consortium led by Vialto Consulting
Project contacts:
18 Goce Delcev Blvd (14th floor)
1000 Skopje
+389 2 3230 635 ext.116

ANNEX TO THE MAIN PART

Project funded by the European Union

Project implemented by Consortium led by Vialto Consulting
Project contacts:
18 Goce Delcev Blvd (14th floor)
1000 Skopje
+389 2 3230 635 ext.116

ANNEX TO THE MAIN PART

Project funded by the European Union

Project implemented by Consortium led by Vialto Consulting
Project contacts:
18 Goce Delcev Blvd (14th floor)
1000 Skopje
+389 2 3230 635 ext.116