THROUGH DIALOGUE TO EU

PRIVACY PROTECTION AS INTEGRAL PART OF DEVELOPING QUALITY E-SERVICES AND TOOLS

This project is financed by the European Union

EU with YOU

FOUNDATION ФОНДАЦИЈА OPEN ОТВОРЕНО SOCIETY ОПШТЕСТВО MACEDONIA МАКЕДОНИЈА

Center for Civil Communications
Центар за граѓански комуникации

REACTOR
research in action

ЕВРОТИНК ЦЕНТАР ЗА ЕВРОПСКИ СТРАТЕГИИ
CENTER FOR EUROPEAN STRATEGIES EUROTHINK

These policy documents are developed to help the civil society organizations and, generally, the citizens, to engage in informed debate and to have access to expert knowledge, opinions and views on topics relevant for EU integrations. Areas in which the Republic of North Macedonia will lead the accession negotiations are both complex and diverse, while reforms to be taken by the country will open numerous dilemmas that require expert debates. Contents created within the project “CSO Dialogue – Platform for Structural Participation in EU Integration” are available on the website: **www.dijalogkoneu.mk.**

- Author: Elena Stojanovska

- This document is avaliable only online

This publication was produced with financial support of the European Union.
Its contents are the sole responsibility of the authors and do not
necessarily reflect the views of the European Union.

PRIVACY PROTECTION AS INTEGRAL PART OF DEVELOPING QUALITY E-SERVICES AND TOOLS

Introduction

In the past several years, the trend of digital services offered by institutions for citizens is marked by a continuous rise. Some factors contributing to the increasing number of e-services include greater availability and more frequent use of the internet among citizens, the need for institutions to demonstrate transparency and accountability, and the fact that the Republic of North Macedonia has joined the EU's Digital Public Administration Programme. From March 2021, living and doing business at the time of global pandemic has imposed the need for portion of existing e-services to be updated and for development of completely new e-services aimed to facilitate communication between citizens and institutions.

A key aspect in introduction of e-services by the institutions concerns regulation of protection of personal data relating to citizens that use such services. Different institutions offer different types of e-services for and communication channels with citizens, thus making it necessary to find the right models for systems of personal data protection and security. Common denominator for all e-services that should be taken into account by all institutions is the need to secure continuous supervision of technical and organizational measures they implement in respect to protection of personal data relating to citizens that are subject of their processing operations.

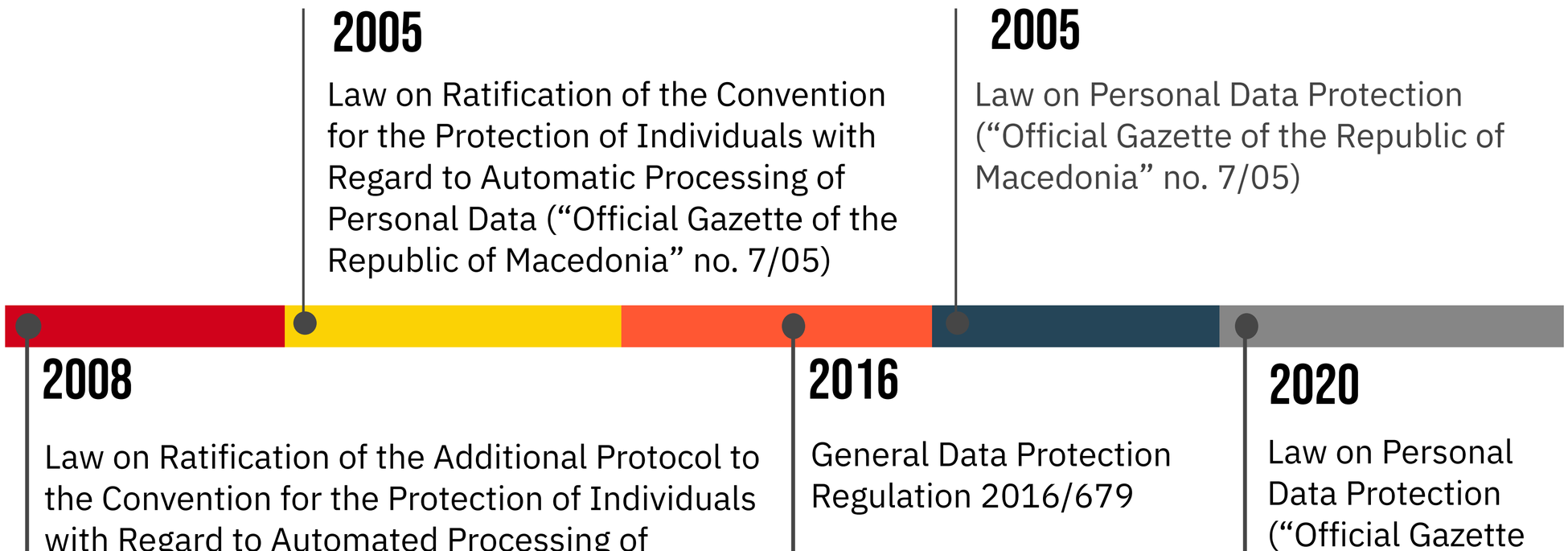
This policy document provides an overview of the standards on personal data protection, as stipulated under the Law on Personal Data Protection ("Official Gazette of RNM" no. 42/20) and the General Data Protection Regulation (GDPR), in respect to planning, creating and introducing e-services by institutions, and challenges standing on the path of the institutions in introducing such standards.

1. Alignment of the national legislation in the field of personal data protection with the EU acquis

In the Republic of North Macedonia, the concept of privacy protection was first introduced in 2005 with the adoption of the Law on Personal Data Protection ("Official Gazette of RM" no.7/05).[1] Adoption of this law has clearly confirmed the country's commitment to align national legislation on personal data protection with the Directive 95/46 of the European Parliament and of the Council on the protection of individuals with regard to processing of personal data and on the free movement of such data,[2] the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data,[3] and the additional protocol to this convention.

Throughout the years, implementation track record of the Directive 95/46 and of national laws on personal data protection, information technology advancement, widespread use of the internet, and development of international businesses have given rise to the need for individuals to have greater control over their personal data. As a result, the General Data Protection Regulation was adopted in 2016 (GDPR 2016/679).[4] This regulation entered into effect in May 2018 and represents a binding document for all EU member-states and countries that process personal data of individuals who are EU citizens.

For the purpose of further alignment with EU regulations, in February 2020 the Republic of North Macedonia adopted a new Law on Personal Data Protection ("Official Gazette of RNM" no. 42/20)[5] that implied a transitional period for full application in duration of 18 months, i.e. the law enters into effect on August 24th, 2021. The new Law on Personal Data Protection is fully aligned with the General Data Protection Regulation 2016/679, accounting for partial attainment of the strategic goal no.1 ("Republic of Macedonia is recognized as country that ensures adequate level of personal data protection") under the Strategy on Implementation of the Right to Personal Data Protection in the Republic of Macedonia 2017-2022.[6] Full attainment of this strategic goal is expected in the upcoming period, by adopting relevant secondary legislation and aligning sectoral laws with the Law on Personal Data Protection.



[1] Available at: https://www.dzlp.mk/sites/default/files/pdf/Zakon_za_zastita_na_licnite_podatoci_2005.pdf
[2] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046
[3] Available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37
[4] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=EN
[5] Available at: https://dzlp.mk/sites/default/files/u4/zakon_za_zastita_na_licnite_podatoci.pdf
[6] Available at: https://dzlp.mk/sites/default/files/dzlp_strategija_mk.pdf

2. Digitalization: condition for provision of quality services and greater transparency of institutions

Implementation of its digital agenda is a priority of the Government of the Republic of North Macedonia. Strategic development and importance of this agenda is confirmed by a series of strategies and action plans in the field of digitalization, such as:

- National Strategy for Sustainable Development of RM 2009-2030
- National Strategy for Information Society Development
- Strategy on Implementation of the Right to Personal Data Protection 2017-2022
- National Strategy on Cyber Security in RM 2018-2022
- Transparency Strategy of the Government of RNM 2019-2021
- National Operational Broadband Plan 2019-2029

Some of these strategies are closely linked to implementation of the Digital Agenda for the Western Balkans, adopted in 2018 as part of the EU enlargement strategy for this region. Main areas covered by this agenda include: reducing roaming charges, broadband, e-government, e-procurements, e-health and digital skills, capacity and confidence building for cybersecurity and digitalisation in parallel to efforts on boosting digital economies, and adopting, implementing and enhancing the acquis system.

In 2020, the Ministry of Information Society and Administration has signed an agreement on accession of the Republic of North Macedonia to the European Union's Digital Public Administration Programme – ISA2. It is a matter of the EU's central programme that supports activities for ICT development in the public administration, provision of electronic services, and digitalization in the public sector. Once this programme is completed, it is expected to be transformed into a more comprehensive programme called Digital Europe that will deal with future standards and guidelines for digital agenda development, while the Republic of North Macedonia would take active part in defining future solutions and standards.

3. Trends in development and availability of e-services

According to the Analysis of Available Electronic Services from April 2020,[7] developed by the Center for Change Management, the Republic of North Macedonia offers a total of 136 administrative electronic services provided by 19 institutions and available on the designated web-portal www.uslugi.gov.mk. Among the total number of available services, 32 percent are fully provided through this web-portal (www.uslugi.gov.mk), while in the case of 68 percent of services the web-portal only offers information and hyperlinks to other (external) portals where actual service provision is enabled. Services available on the web-portal and marked by frequent use on the part of citizens concern issuance of personal identification documents and identity cards, and services related to health insurance, education, social protection rights, taxes and life events.

Securing electronic means for provision of such services is more frequently noted among a number of municipalities as well. Examples thereof include mobile application "mCommunity", the web-portal of the City of Skopje's Technical Support Center for Submitting E-Application,

[7] Available at: https://cup.org.mk/publication/9036_Analiza-na-dostapnite-elektronski-uslugi.pdf

and a number of websites hosted by individual municipalities where citizens are able to receive e-services. Most often, citizens are able to make proposals, lodge complaints, submit applications for subsidies, construction permits, and report problems.

In addition to e-services offered on the web-portal www.uslugi.gov.mk and e-services offered by local self-government units, especially popular are e-services and tools that are additionally offered to citizens, such as: mobile application for value added tax refund – MyVAT, web-portal on expressing interest for vaccination against COVID-19 - www.vakcinacija.mk, mobile application for location of persons infected with COVID-19 - StopCorona, and web-portal for online education support - Eduino.[8]

There is a crucial difference among services offered on the web-portal www.uslugi.gov.mk, e-services provided by local self-government units and other services enlisted above.

E-services incorporated on www.uslugi.gov.mk and e-services provided by local self-government units represent an alternative to provision of in-person services, but they do not constitute an additional service which citizens would not be able to receive otherwise. All services featured on this portal are actually services which citizens can also receive in physical, i.e. written form. They are closely related to rights enjoyed by citizens under sectoral laws that clearly stipulate procedures for exercise of such rights, scope of data required for service provision, competent authorities providing such services, deadlines for service provision, and the like.

E-services like MyVAT, www.vakcinacija.mk, StopCorona, and Eduino are services available to citizens only in electronic form and cannot be obtained in any other manner. Institutions that created these e-services have law-stipulated competences to offer them, but at the same time there are no law-stipulated procedures that regulate the manner in which services are provided.

4. Protection of personal data of users: key imperative for quality e-services

Pursuant to the Law on Personal Data Protection, institutions act as controllers[9] of personal data collections (filing systems) and should align their operations with provisions from this law by establishing a system of personal data security and protection. The system of personal data security and protection should provide detailed definition of collections (filing systems) that are subject of personal data protection, technical and organizational measures for personal data protection, authority granted to persons engaged in processing of personal data, relations with third parties that, on behalf and for the account of the institution, are processing or using personal data that have been initially processed by the institution in question. The system of personal data security and protection must also define the manner in which citizens, i.e. data subjects[10] are able to exercise their rights arising from the law.

---

[8] The criterion for selection of above-enlisted e-services and tools is frequent use thereof by citizens, especially in the last year, i.e. during the Covid-19 pandemic.
[9] Controllers shall be any natural or legal person, state administration body or legal entity founded by the state for performance of public authority, agency or other body which, independently or together with other entities, determines the purposes and the method for personal data processing, and where the purposes and the method for personal data processing are stipulated by law, the same law should also determine the controller or the specific criteria for its determination.
[10] Data subjects shall be any natural person whose identity can be determined, directly or indirectly, especially on the basis of identifiers such as: name and surname, single identification number, location data, identifiers on the internet, or on the basis of one or several features that are specific to their physical, physiological, genetic, mental, economic, cultural or social identity.

4.1. Principles of personal data processing

In its alignment process, each institution should start by assessing whether it complies with the principles of personal data processing that are clearly defined in the Law on Personal Data Protection.

- **Lawfulness, fairness and transparency:** personal data shall be processed pursuant to the law, to the sufficient extent, and in transparent manner;
- **Purpose limitation:** personal data shall be collected for specific, clear and legitimate purposes and shall not be processed in a manner that is incompatible with such purposes;
- **Data minimisation:** personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- **Accuracy:** personal data shall be accurate and, where necessary, kept up to date, and all reasonable measures shall be taken for deletion of inaccurate or incomplete data, having in mind the purposes for which they are processed;
- **Storage limitation:** personal data shall be kept in the form that allows identification of data subjects, but not longer than the period necessary for the purposes for which they are processed;
- **Integrity and confidentiality:** personal data shall be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, by implementing adequate technical or organizational measures;
- **Accountability:** controller shall be responsible for their compliance with the Law on Personal Data Protection and shall be obliged to demonstrate such compliance.

4.2. Lawfulness of personal data protection when using e-services

In defining terms and conditions for use and functionality of e-services, each controller introducing e-services should start with clear definition of lawfulness for processing of personal data of citizens (data subjects) when using these services.

Processing based on law-stipulated procedures

Processing of personal data through use of e-services available on the web-portal www.uslugi.gov.mk and e-services provided by local self-government units is regulated by means of law-stipulated procedures on the method for service provision (examples thereof include submission of applications for issuance of personal identification documents, birth certificates, applications for subsidies, lodging complaints, reporting problems and the like).

What is specific in this case is the fact that the institution receives such applications in electronic form, and later creates a docket and continues with the procedure for service provision pursuant to the law under which the relevant service is provided (e.g., Law on Identity Cards, Law on Motions and Complaints, Law on Health Insurance).

In such case, the controller is required to additionally regulate the legal ground for personal data revealed by citizens (data subjects) as part of their registration on web-portals or mobile applications. Data for registration on any electronic portal represent a new personal data collection (filing system) that is not anticipated by law, and therefore the institution is obliged to ensure legal ground for its existence/creation. In this specific situation, the legal ground is consent from citizens (data subjects).

Processing based on consent

E-services like MyVAT, www.vakcinacija.mk, StopCorona, and Eduino are services available only in electronic form and citizens cannot obtain them in any other manner. Institutions that created such e-services have law-stipulated competences to offer them, but at the same time there are no law-stipulated procedures on the manner in which these services are provided.

Use of these e-services is conditioned with the citizen's registration and disclosure of their personal data needed for the service to be made available to them. The electronic database created from use of these e-services represents a new personal data collection (filing system) and each institution should take into account the manner in which technical and organizational measures for personal data security and protection are applied in respect to processing of personal data from such collections. In this case, the only legal ground is a consent provided by citizens in order to use the relevant e-service.

When data processing is based on consent, the controller is obliged to demonstrate that data subjects have given consent to processing of their personal data, i.e. to possess electronic proof demonstrating that the concerned data subject has consented with the privacy policy and the terms and conditions for use of e-services.

Data subjects have to right to withdraw their consent at any time. The withdrawal of consent does not affect lawfulness of processing that had been based on consent given prior to its withdrawal. The action for withdrawal of consent must be equally simple as the action for giving consent.

5. Transparent information: a requirement for setting up e-services

Provision of open information on personal data processing, made available on the location where e-services are based is a legal obligation for all controllers that offer e-services. Privacy notice is the basic document that contains all information needed by data subjects prior to the start of using e-services. In addition to providing a complete overview of the manner in which e-services are used and personal data processing operations, the privacy notice is of key importance in ensuring that consents given by data subjects are based on previous information.

In order to be considered complete, the privacy notice must provide answers to the following questions:

5.1 Who is who?

First information that should be elaborated under the privacy policy/notice concerns the controller of personal data collection (filing system), i.e. who has created or who owns the platform, application, e-tool. This information should include the name of the controller (institution) and contact details. In addition, it should also include information on name and surname and contact details for the personal data protection officer.[11]

5.2 What are the purposes of personal data processing and what is the legal ground for processing?

The purposes of personal data processing through use of e-services should be provided in clear, specific and easily understandable manner for users. The controller should inform that personal data would not be used for any other purposes different from those initially defined. In addition,

[11] The personal data protection officers shall be appointed on the basis of their professional qualifications, in particular their professional knowledge of the legislation and practices in the field of personal data protection, as well as their ability to perform tasks and duties arising from the Law on Personal Data Protection.

it should be indicated whether these purposes are linked to the controller's legal obligation (e.g., for issuance of identity cards pursuant to the Law on Identity Cards). In the case where the purposes of personal data processing through use of e-services are related to processing based on consent (e.g., for the purpose of expressing interest for vaccination against Covid-19), it should be clarified that the consent serves as legal ground for processing. By providing such information, the controller ensures transparent information on the manner in which it complies with the principle of lawfulness, fairness and transparency, and the principle of purpose limitation.

5.3. Which categories of personal data are processed?

Categories of personal data that are processed should be enlisted in details. Clarification on the categories of personal data that are collected about users of e-services should take into consideration whether personal data required for use of relevant e-service are clearly indicated and which personal data are revealed by users on their free will, as well as that (non)disclosure of such data does not affect quality of e-services provided. In this regard, it is of key importance to provide information that would indicate to the fact that personal data are adequate, relevant and limited only to those necessary for the purposes for which they are processed.

5.4. How are personal data protected?

The controller should made known that it has defined adequate technical and organizations measures in order to ensure protection of personal data that are processed through use of e-services. Safeguards in this respect concern protection against unauthorised access, unlawful disclosure, accidental loss, destruction of data, levels of user verification, encrypting. It should be clearly noted that access to personal data is limited only to persons with special authority and those responsible for personal data processing.

5.5. What are the deadlines for storage of personal data?

The controllers should pay serious attention to setting deadlines for storage of personal data that are processed for the purpose of using e-services and should provide clear information thereof in their privacy notice. In the case of services related to law-stipulated procedures, deadlines anticipated in the list of document materials with deadlines for their storage shall be applicable for each institution separately. These deadlines are easily identifiable because they are regulated under provisions from relevant laws and the Law on Archival Materials, whereby the institution should only anticipate the procedure for data deletion and/or destruction upon expiration of relevant deadlines.

In the case of personal data that are processed on the basis of consent, such as data for registration of user profile and data for obtaining services that are not subject of law-stipulated procedure, the storage period is closely related to the user's consent. Should the user decide to withdraw its consent, the controller is obliged to delete their personal data.

5.6. Are personal data disclosed to processors or users?

In many cases, in addition to the controller that has created the relevant e-service, access to personal data is granted to another institution that is somehow involved in service provision. These relations need to be clearly presented in the privacy notice for users to be informed about who, and for which purposes, has access to their personal data. For example, the web-portal www.uslugi.gov.mk is created by the Ministry of Information Society and Administration, but used by other institutions to offer services, while registration of new user profile is redirected to subdomain that contains the name of private company. What is missing here is clear information about which entity from those involved in the process has what role pursuant to the law, does the private company serve as data processor, do other institutions act as controllers, but only of data needed for provision of services, does the Ministry of Information Society and Administration have access only to data from user profiles. All these relations need to be regulated under separate agreements on personal data processing.

5.7. Is there an automated decision-making process, including profiling?

Institutions-controllers should provide information on functionalities of the electronic tool, the system used for service provision, and should enlist whether it performs automated connection of users and whether it uses profiling function.

5.8. What are the rights of data subjects?

Right to information (Art. 17 and 18 of LPDP)	Controllers are obliged to inform data subjects about personal data collected for them, purposes for personal data processing, periods for storage of personal data and whether personal data are disclosed to third parties. Also, controllers are obliged to post such information on their websites, at their business premises or provide data subjects with such information in hardcopy or electronic form.	Deadline: at the moment when the processing of personal data starts.
Right to access (Art. 19 of LPDP)	On request from data subjects, the controllers are obliged to provide them with detailed information on processing of personal data relating to them.	Deadline: one month from the day when the request was submitted and three months in the case of complex requests.

Right to rectification (Art. 20 of LPDP)	On request from data subjects, the controllers shall rectify or complement any inaccurate or incomplete personal data relating to them.	Deadline: 15 days from the day when the request was submitted.
Right to erasure (Art.21 of LPDP)	On request from data subjects, the controllers shall erase personal data when the purpose for which they were processed is attained, when the data subject has withdrawn its consent to personal data processing, when personal data had been subject of unlawful processing, when the data subject has objected to personal data processing, and for the purpose of compliance with the controller's obligation for deletion of personal data when there is no valid legal ground for personal data processing.	Deadline: 30 days from the day when the request was submitted.
Right to restriction of processing (Art. 22 of LPDP)	On request from data subjects, the controllers shall restrict personal data processing when the data subject has objected to accuracy of personal data, until accuracy of data is confirmed, when the data subject believes the processing is unlawful, but objects to data deletion, or when personal data relating to them are needed for exercise of legal claims.	Deadline: one month from the day when the request was submitted and three months in the case of complex requests.
Right to data portability (Art. 24 of LPDP)	On request from data subjects, the controllers shall transfer their personal data in a structured, commonly used and machine-readable format or shall transfer then to another company. This right is applicable only in the case of personal data processing based on consent or agreement and in the case of automated processing.	Deadline: one month from the day when the request was submitted and three months in the case of complex requests.

Right to object (Art. 25 of LPDP)	On the basis of complaint submitted by data subjects, the controllers shall discontinue processing of personal data for the purpose of direct marketing or profiling related to direct marketing.	Deadline for action: one month from the day when the request was submitted and three months in the case of complex requests.
Right not to be object of automated decision-making (Art. 26 of LPDP)	Data subjects have the right to request not to be object of decisions based on automated data processing, decisions based on profiling, when such decisions create legal consequences for them. The controllers must not make such decisions when the data subject has submitted written request not to be object of automated decision-making.	Deadline: one month from the day when the request was submitted and three months in the case of complex requests.
Right to withdraw consent (Art. 11 of LPDP)	On request from data subjects, the controller shall discontinue processing of personal data relating to them. The withdrawal of consent does not affect lawfulness of personal data processing that had been performed on the basis of such consent prior to the withdrawal.	Deadline: immediately.

6. Personal data protection officer

One of the more important changes under the new Law on Personal Data Protection concerns the enhanced role of personal data protection officers. According to past practices, persons employed to another job position were appointed as personal data protection officers and were assigned additional tasks and duties arising from the Law on Personal Data Protection. Such practice might have been proved as good thus far, but the scope of work tasks and duties and the position of these officers under the new law raise the question whether this practice could continue in the future, especially in the case of institutions with large number of personal data collections (filing systems), personal data of large scope, and additional e-services for citizens.

In order to ensure efficiency in performance of their obligations, the controllers are obliged to make sure that personal data protection officers are adequately and timely involved in all issues related to personal data protection and to provide them support in performance of their tasks and duties by ensuring they have all resources necessary and access to personal data and processing operations. Moreover, the controllers should guarantee that officers would not receive any instructions from top management in respect to performance of their tasks and duties.

In addition to the above enlisted, the institutions should ensure continuous education for these officers in order to make sure that, in performing their tasks and duties, they are prepared to take into account all risks related to processing operations, as well as the scope, context and purposes of personal data processing.

Personal data protection officers are responsible:

- to inform and advise employees engaged in personal data processing about their obligations;
- to monitor compliance with the law, with other laws relating to personal data protection in the Republic of Macedonia, as well as the controller's internal policies on personal data protection;
- to allocate responsibilities, raise awareness and train employees engaged in processing operations, and to perform audits on personal data protection;
- to provide advice in relation to impact assessment on personal data and to monitor performance of such assessments;
- to cooperate with the Agency for Personal Data Protection.

7. RECOMMENDATIONS

In order to provide quality e-services that would facilitate communication with citizens, while ensuring privacy protection as integral part and functional element of their systems, the institutions are recommended:

01 To develop the methodology for assessment of priority e-services and dynamics of its development. The number of e-services is not proportional to their quality, and therefore, instead of moving towards mass digitalisation, an assessment should be made on which services and which categories of citizens are priority and how can these be adequately developed and made available.

02 To review the existing internal acts on personal data protection, to conduct needs assessment for alignment with the new Law on Personal Data Protection and to conduct assessment of internal human resource, technical and financial capacity that could be used for implementation of the alignment process.

03 To conduct analysis of privacy risks for each e-service or tool they are creating. The analysis would provide clear guidelines on the manner in which privacy protection should be integrated during creation of e-services or tools. By doing that, the institutions would have integrated from the very start the principles of personal data security and protection for new collections (filing systems) that arise from use of e-services.

04 To provide transparent information on personal data processing for use of e-services or tools at the location where services or tools are made available. Moreover, they need to ensure easy and streamlined exercise of the rights of citizens as data subjects.

05 To appoint personal data protection officers who are professionals in this field or to provide them with quality education and support for performance of their tasks and duties. In addition, employees engaged in personal data processing need to be continuously educated on application of the law and relevant internal acts.

06 To work on raising awareness and digital literacy as key preconditions for mass and adherent use of e-service and tools by citizens.