METAMORPHOSIS

LAWS IN MACEDONIA

Adherence to Data Protection Principles

LAWS IN MACEDONIA

Adherence to Data Protection Principles

Publisher:
Metamorphosis Foundation for Internet and Society
postol Guslarot 40, 1000 Skopje, Macedonia
www.metamorphosis.org.mk
info@metamorphosis.org.mk
tel./fax: +389 2 3109 325

About the publisher:
Bardhyl Jashari

Research team:
Elena Stojanovska – Head researcher
Bardhyl Jashari
Filip Stojanovski
Goce Arsovski

Translated by:
Kire Dimic

CIP - Каталогизација во публикација
Национална и универзитетска библиотека „Св. Климент Охридски“, Скопје

342.738:340.13(497.7)

LAWS in Macedonia : adherence to data protection principles / research team Elena Stojanovska ... [и др.] ; translated by Kire Dimic]. - Skopje : Metamorfozis, 2015. - 36 стр. : граф. прикази ; 21 см

Библиографија: стр. 36. - Содржи и: Annex

ISBN 978-608-4564-62-1

а) Заштита на лични податоци - Правна рамка - Македонија
COBISS.MK-ID 100070666

CONTENTS

Privacy is one of the major challenges we are facing as users of information and communication technologies (ICTs) in everyday communication and in our work. The rapid development of ICT has dramatically changed the way personal information is collected, stored, accessed and shared. Regardless of the area in question, whether it's health, social welfare, banking or just ordinary online communication, today a vast quantity of personal data is stored in digital format that provides easy and cheap access, recording and distribution. However, this also drastically increased the possibility for privacy violations. Today, this can be done by individuals, private companies, as well as government institutions and agencies.

To protect the privacy of citizens, governments throughout the world adopted various laws and policies. Unfortunately, the proposed legislation and policies are often ineffective due to the lack of clear and universal understanding of the very concept of privacy and the ineffficiendt implementation. Very often, in the name of safety and security of citizens, governments deregulate the balance between freedom and privacy.

This project is an attempt to provide insight into how 35 laws from 12 areas in Macedonia adhere to the general principles of privacy and personal data protection and thereby to contribute to their compliance with the EU's privacy standards and principles.

We at the "Metamorphosis" Foundation support laws, corporate policies and technologies that protect the privacy of citizens, and we also advocate for greater legal control and supervision of the government institutions that are authorized to eavesdrop, in order to prevent misuse of these authorizations.

Bardhyl Jashari,

Director,
Metamorphosis
– Foundation for Internet and Society

SUMMARY

The research of the legal and institutional frameworks in Macedonia in terms of privacy aimed to evaluate the current situation and opportunities offered by these frameworks for the protection of citizens' individual privacy. The research also provided a reference framework and methodology for conducting future researches and projects in this field.

The identification of laws and bylaws affecting the right to privacy – particularly the ones regulating the personal data collection, processing, transfer and storage, can actually help citizens (who are not legal experts) to easily identify the methods, laws and institutions that may compromise their privacy.

Research Results

Experts are unanimous that the protection of personal data and citizens' privacy is just as important as raising the citizens' awareness about their privacy. They also agree that the legislation guaranteeing personal data protection, and the projected technical and technological measures in Macedonia are satisfactory, but according to the experts, the problem lies in the application of the laws.

Experts believe the situation with privacy in Macedonia is not quite satisfactory, although it is constantly improving. They identified several methods and target groups that we need to focus on, because the situation with the protection of privacy and personal data is a societal problem that must not be ignored.

The analysis of the laws indicates that a number of laws do not stipulate clear and specific deadlines for the period of storing citizens' personal data. Also, a request for consent for data collection is not stipulated in most of the laws regulating personal data collection, and there are also laws failing to meet almost all of the criteria for protection of privacy and personal data.

According to the analysis, there are also laws that comply with the principles of the Law on Personal Data Protection, prescribing specific deadlines and purposes for personal data collection, i.e. fulfilling the criteria of the law analysis, and complying with EU recommendations.

The analysis resulted with recommendations for various areas and specific laws. These recommendations indicate the need for introducing amendments to some of the articles of these laws, or for introducing new articles, thereby guaranteeing the privacy of the citizens when their personal data is being collected, stored, processed and transferred in accordance with these laws.

INTRODUCTION

The quick rise of technology in people's lives, and its penetration in all interactions of the average citizen makes it an extremely powerful tool in the development of the culture of societies.

However, when it falls into the wrong hands, technology and its ubiquitous presence in people's lives is a dangerous weapon, which can (with extreme precision, specific methods and techniques) inform us about the complete communication, geographical location, financial history etc., for a certain person or groups of interest.

Of course, these opportunities offered by technology, are not inherently threatening the quality of life of the average citizen, i.e. the common use of such technology is intended for marketing purposes, which in turn may be positively perceived by the end user - the citizen.

But the following question comes to mind - who decides where and how exactly the technology used to identify its users can have access to this information anytime? Is the average user aware of the transfer of his personal data, such as photos, financial history, geographical location, which is performed on a daily basis through various communication channels between public and private institutions and corporations?

Today, more than ever, the average user needs to manage their virtual presence - the quick development of new identification techniques (by pressing a button, by briefly looking into the camera lens) also carries an increased risk for misuse of their information. Personal responsibility and obtaining information about each separate service is a crucial step for privacy protection.

On the other hand, aside from the users' personal responsibility for managing their virtual presence and provision of personal data, the legal regulations on a global and national level are a very useful protection measure. The right to privacy and private life is a globally recognized human right, and as such it is subject to compulsory acceptance by all states - signatories of the Declaration of Human Rights.

Laws and bylaws can do so much in terms of protection of privacy and personal data of citizens, by limiting, monitoring, and punishing private companies and state institutions that are using this data in their daily operations. Therefore, as companies are becoming more innovative in the collection, storage, and transfer of personal data – regulations should follow at the same pace, protecting the citizens and their right to privacy in each of the steps of processing citizens' data. States have an obligation to create an appropriate legal infrastructure that will protect the privacy of citizens, and protect it from the government institutions.

There is a great need for an entity that will monitor and control big companies and public bodies in their use of citizens' personal data. Such organization, body or commission, will have the opportunity to propose amendments to the regulations,

warn about possible privacy violations, punish where there is misuse of personal data, implement appropriate measures and techniques for raising the awareness among the citizens about the risk of misuse of their personal data.

In our country, that body is the Directorate for Personal Data Protection (DPDP).

It was formed in 2005 with the adoption of the Law on Personal Data Protection, which largely contributed to comply with global and European trends in the field of human rights, especially the right to privacy.

In 2008, the Law Amending the Law on Personal Data Protection was adopted, as a law that promotes the pro-European steps of Macedonia in the harmonization with the legislation of the EU member states. The Directorate for Personal Data Protection is a place where the citizens of the Republic of Macedonia can turn if they have reason to believe that their personal information is being misused, stored for longer than planned, changed, are inaccurate or being transferred to third parties – without an explicit permission from the citizen. The Directorate for Personal Data Protection is required to initiate an investigation procedure conducted by its controllers (stipulated in the law) who have a legal obligation to investigate using technical and other measures, if there was indeed an unlawful use of the data.

During the past few years, the DPDP received a number of reports on possible misuse of citizens' personal data (reports are available on the DPDP website), and is further handling the eligible reports. However, if we take into consideration the number of reports, we can conclude that the awareness about this issue is low among the general population. The public is not familiarized with the methods of storage and use of personal data, which they are easily disclosing to private companies. The public is also not familiarized with the legal mechanisms for protection from this kind of illegal personal data collection, and the possibility to address the relevant parties that would help them in the event of negative consequences from the publication of such data.

Therefore, the aim of this project is to raise public awareness about the rights and laws protecting their personal information - and where to turn if they suspect that their personal information is misused.

LEGAL FRAMEWORK FOR PRIVACY

Macedonia has its own legal framework that guarantees the right to privacy and protection of personal data. Article 25 of the Constitution states:

> *"Every citizen is guaranteed the respect and protection of the privacy of personal and family life, dignity and reputation."*

Article 18, however, says:

> *"The safety and confidentiality of personal data is guaranteed."*

> *"Citizens are guaranteed protection from infringement of personal integrity arising from the registration of personal information through data processing."*

The Constitution protects the privacy and freedom of communication: Article 17 states:

> *"The freedom and secrecy of correspondence and other forms of communication is guaranteed. Only a court decision may deviate from the principle of inviolability of the secrecy of correspondence, if necessary for a criminal investigation or it is in the interests of the defense of the Republic."*

Finally, Article 26 guarantees the inviolability of the home:

> *"The inviolability of the home is guaranteed. The right to inviolability of the home may be restricted only by court decision in the detection or prevention of crime or the protection of human health."*

Apart from the legal framework provided in the Constitution, there are additional laws and regulations in Republic of Macedonia that promote the protection of citizens' personal data and their privacy.

The Law on Protection of Personal Data, adopted in 2005, defines the ways in which citizens' personal data is collected, when the collection and storage of personal data is allowed and when it is not, it defines categories of personal data based on sensitivity, and also measures to protect them from illicit processing.

Generally, citizens' personal data may only be processed with the express consent, except in cases of great importance for the security of the country.

Furthermore, the law specified technical measures necessary for the physical security of databases. In the period after the initial adoption of the law in 2005, guides and handbooks were made which further specified the necessary technical measures for institutions to collect, store and / or process personal data, which further contributes to the security of the data.

In recent guides, the latest available now dated 03.2014, there are listed administrators of databases, which have obligations prescribed by law, such as

maintenance of databases, providing the servers that store data technical measures for physical security and protection from external influences, approving and creating access through passwords to employees who use such data in daily operations, multiple levels of authorization etc.

With the latest guides and bylaws, we notice a trend of following and specifying the regulations concerning the protection of personal data and the right to privacy with the widely accepted proposals by the EU and the global scene.

Besides the above mentioned constitutional and legal provisions that promote privacy and protection of personal data, there are a number of other laws and regulations that belong to certain sectors (such as the Law on State Statistics and the Law on Social Protection) that further ensure this basic human right. Because the police authorities, the employment agency, pension insurance, etc., use (collect, store, process) personal data in their daily operations, it is necessary in such instances to further specify the ways in which this data will be used, as well as mechanisms for protection from misuse.

The EC Progress Report on the Republic of Macedonia, published by the European Commission on October 8, 2014, noted the following conditions and needs:

> *„The Directorate for Personal Data Protection additionally increased the number of inspections, 60% of which were conducted in the private sector and 40% in the health sector and judiciary. Almost half of these inspections confirmed infringements. The number of complaints submitted to the Directorate was 404 in 2013, out of which 62 % were related to misuse of data on social networks. In general, the number of revealed and confirmed infringements was increased five times, from 56 in 2012, to 254 in 2013, as a result of the proactive approach of the Directorate. The activities for awareness raising of the public also continued, resulting with a 30% increase of the number of visitors of the Directorate's website. The number of controllers and public servants for data protection has been increased and their training has been improved, although four members of the personnel have left. The Directorate submitted its first report to Eurojustice for personal data protection in the public prosecution system. The legislation for the relevant sector has not yet been harmonized with the legislation on data protection and much more efforts need to be made in order to ensure that the Directorate is systematically consulted about all the new policies and draft-laws. In order to fully comply with the acquis, we need to additionally adjust the legislation on personal data protection."*

RESEARCH METHODOLOGY

The research had two separate stages of data collection - the first stage was conducting semi-structured interviews with experts, while the second phase consisted of a legal analysis of the identified laws that have the potential to violate the right of privacy of citizens.

In the first stage, participants in the interviews were selected on several criteria - their formal education, their experience in the issues that hinder the right to privacy and protection of personal data and daily exposure to a number of personal data of citizens. Although a number of official invitations were sent, at the outset, to state institutions (ministries) to nominate a representative who would participate, we found a low turnout for cooperation - one of eight state institutions agreed to participate in the survey, with the nomination of a representative which satisfy the above criteria.

Half-structured interviews, such as a qualitative method, were selected due to several reasons: they allow a deeper understanding of the views and positions of the experts, and as opposed to other methods, for instance a focus group or standardized interview, half-structured interviews provide a certain freedom in the discussion, in terms of the conversation flow and questions asked, but more importantly, in terms of the "freedom" of expression of participants.

Because the topic of the survey is of a sensitive nature, the use of focus groups or group interviews would prevent certain views of the participants to "surface", due to the presence of other people in the process.

Of course, the generalization of findings from the half-structured interviews is unnecessary, because they provide a perception about the views and positions of the participant, although the formulation of certain statements of the participants includes descriptions for the wider population.

In addition, interview participants filled out a survey questionnaire that contributed to a more objective perception of their views and opinions, and at the same time allowed the views of interview participants from various fields to be easily compared.

Eight interviews were successfully conducted, with an average duration of 25 minutes. As the participants discussed and shared views on a sensitive topic, it was guaranteed that their identity would remain known only to the person conducting the interview, so that they wouldn't face repercussions in their private and professional life.

RESULTS OF THE SURVEY OF THE VIEWS AND OPINIONS OF EXPERTS

Characteristics of the interviewed experts, by sectors

- **2 from the education sector**
- **1 from the civil society sector**
- **1 media expert**
- **1 public relations specialist**
- **1 public enterprise manager**
- **1 from the telecommunications sector**
- **1 from the insurance sector**

The interviews began in the second half of December, 2014. Below is the qualitative analysis of the responses of the experts and attached questionnaire which the interviewed all filled out before the start of the interviews.

*** How important is storage, processing and transfer of personal data of citizens for the daily operations of the institution / organization to which you belong?**

On the first question, all interviewed experts shared the view that the personal data of citizens are essential to the daily functioning of institutions, that is, without the processing and storage of personal data - companies or institutions could not function.

*** How familiar your institution / organization is with the legislation and regulations for the protection of personal data?**

For this question, almost all experts said that their institutions are well familiar with the legislation and regulations. Some experts positively evaluated the work of the Directorate for the Protection of Personal Data in terms of regular training and recommendations that come from them, and assisting in educating their employees about the importance of the protection of personal data and the right to privacy. Also, almost all experts agreed that there is room for improvement in this area, especially among employees, or sectors, which, firstly, have direct contact with customers / clients (and have insight into their personal data) and, secondly, are not part of legal or IT sector in their institution / company (for these two sectors, experts believe that there is great familiarity with the legislation and regulations).

*** In your opinion, is there a risk of disclosure of content in the daily operations of the institution / organization that would violate the privacy of citizens? If such risk exists, what you think could be done to remove or reduce it?**

On this issue, the experts were unanimous: risks always exist, but they are small and insignificant, and continuing work is being done on their rehabilitation. This is achieved through continuous staff training, setting high standards for technical security of the servers and databases where the personal data is stored, as well as monitoring the development of technology and constant replenishment of the rules of procedure. Experts split the risks in two areas - technical risks and risks arising from the employees themselves. They gave the technical risks an insignificant role, ie, they were satisfied by the use of sophisticated tools and security protocols by their IT departments for which they are responsible, while they consider that the biggest room for improvement

is in the part of education of employees, especially new employees. The personal opinion and attitude of the employees (and citizens) to the right to privacy, and the importance of protecting someone else's personal data is at a very low level. In other words, citizens' awareness of this issue is very low and unrepresented in wide circles, and that entails the greatest risk of violation of privacy.

> ***There is always a risk, and I always say that the most important thing is the awareness of the employees. This data actually represents people's wealth, and it should therefore be protected. This is why we are conducting the trainings, and the technical measures for personal data protection taken by the company are just as important as the organizational measures.***

How would you rate the overall climate in your institution / organization in terms of the need for privacy and protection of personal data?

Experts were unanimous on this matter, in the view that all institutions and companies are keeping an eye on citizens' personal data and the protection of their privacy. Some of them have said that in some state institutions, however, this issue is not sufficiently treated, particularly in institutions related to public health, and not much care is being taken into others' privacy, but generally there is a climate among employees in all sectors that personal data is important, and that the right to privacy of citizens should be respected.

How would you rate the awareness of the general public in terms of the right to privacy?

- **How important is the need for raising awareness among the general population of their basic human right to privacy?**
- **Where do you think there is most room for improvement?**

Almost all interviewed experts on the issue agreed that awareness among the general public is very low. The average citizen has little familiarity with his or hers rights in respect of the right to privacy and the use of their personal data, as well as possible damage and consequences thereof. Some experts expressed the opinion that citizens are aware of their rights, but simply do not appreciate their significance and knowingly allow their privacy to be breached.

All experts agreed that the need for raising awareness of the wider population of these basic concepts is a very important one, and some of them thought that through continuous education, especially early, school-age, and with solid family upbringing, future generations can become informed and careful in their decisions, when they come in situations where the right to privacy is potentially threatened. One participant in the interview cited the example how you can act systematically and planned on the employed workforce (whether in public or private companies) – through systematic and planned continuous education on-the-job, for which the financially responsible will be the institution / company itself, the effect of which will not stop in the working environment, but will trickle down in the home environment, the family, because "... as they behave at work, they will pass that same culture at home." After that, it's a short step from the family environment, to the social environment and culture.

...if we allow unauthorized mass collection of personal data, we have a common problem. We have no control over that data and where it can be transferred, maybe even beyond the borders of the Republic of Macedonia. We can do a lot to improve this situation...

On the last sub-point, almost all experts were unanimous that the most room for improvement exists in young people, teenagers and students in primary and secondary schools. With the rapid development of technology and mobile devices, and the multitude of applications for them, as well as social networks, young people are constantly exposed to risk that their personal information be displayed, used, transferred and stored in places and ways that they are not sufficiently informed about (although he or she may have given prior consent). By agreeing to the terms of use of applications and social networks, experts believe that they do not know enough to decide to what extent to "trade" their privacy and personal data.

Have you personally been in a situation where your right to privacy has been denied? If yes, what did you do?

Interviewed experts were divided on this issue - almost half of them said they never felt that they were denied the right to privacy, while the other half confirmed that, almost on a daily basis, their right to privacy is being violated. However, the group that responded with confirmation, attributed the cases of violation of their privacy to negligence of employees in certain institutions / companies, i.e., more random than with the intention of causing harm. Because of this, none of the experts who said that their right to privacy was violated decided to act in those situations. Besides random errors and embarrassment, several experts said they were victims of "spam" by certain private companies, through SMS, email, phone calls, etc., even though they did not give consent. They reacted accordingly to these procedures, and further communication was interrupted.

Which institutions / agencies / organizations that hold, use, and process your personal data are you aware of?

The above question we used to paint a picture of, what is the level of awareness among the expert public, which on a daily basis deal with this issue, for the use and storage of their personal data in relation to the public. In that context, the experts, with the exception of one participant, confirmed our assumption that they will be very well aware which institutions / companies possess their personal data. With the exception of one participant in the interviews, which only managed to enumerate three institutions that he/she is familiar that have and use his/hers personal data, other experts enumerated more than 10 private companies and institutions that currently have and use their personal data.

How do you evaluate the role of new technologies in terms of the right to privacy of citizens?

The experts were agreed on several points of this issue:

They shared the view that new technologies carry a large potential for invasion of privacy on their users;

Technology very quickly penetrates in the everyday life of the citizens, more quickly than he /she is ready to learn, in the short time given, on the risks associated with their use;

Hence, the need for continuous education and information when making decisions about the techniques and technology used in everyday life becomes a particularly important issue, and

Technology is only a tool that can be used to protect one's privacy and personal data, as much as it can be used to violating it – the intentions of the person who uses the technology remain as one of the most important factors in determining whether new technologies are positive or negative relative to the citizens' privacy.

How do you evaluate the role of the Internet, specifically social networks, in terms of the right to privacy?

The experts were unanimous in the view that social networks and the Internet play an irreplaceable role in today's society and social functioning. These satisfy the appetites of many people for socializing and expanding contacts and a wealth of information.

However, experts also said that most of the cases in private life, from contacts with friends and acquaintances, where there was violation of one's right to privacy and/or misuse of personal data - came from social networks. Therefore, they agree that the use of social networks is a doubled-edged sword - there is a big risk for violation of privacy, but they also carry great benefits. As to the reasons for this daily invasion of the privacy on social networks, the experts attributed:

Insufficiently informed users accepted terms of use and their contents;

Too complicated instructions for setting "level of privacy" of information that users share, and

Lack of information about potential risks and possible consequences of careless use of social networks and their contents.

For the last item, one of the experts expressed particular concern about the lack of awareness among the young population, i.e. students in primary and secondary schools. Because many of these students actively use social networks and the Internet on a daily basis, the risks of violation of their, and other people's privacy is great.

Where do you think there should be exceptions to this basic right, i.e., when it is better to allow invasion of privacy and use of personal data without explicit consent? Which institutions would have this right?

Experts agreed that there should be exceptions where the privacy of citizens, or a group of citizens could be compromised, however:

Each of these exceptions should be provided by law;

The social networks are necessary, they are powerful tools for social activity and for satisfying people's needs for socialization... But they can also easily be used for a violation of privacy.

Only certain institutions would have that right, and in addition, certain sectors inside these institutions;

Each case of violation of someone's privacy to be evaluated separately, i.e., to assess whether it is really necessary, and

The most important prerequisite to even think about monitoring one's activities, phone calls, bank accounts, etc., is when there are serious indications that the person or group is involved in acts against national security. If there are criminal charges already in place, and proven criminal acts, also, the right to privacy of the culprit(s) would be violated, or rather, temporarily suspended, so as the judicial authorities and the public prosecutor could carry out their legal obligations. Experts also agreed that institutions such as – the police, courts, prosecutors, IRS and emergency centers, would have this right.

*** How do you evaluate the situation with the privacy and protection of personal data in Macedonia? How do you evaluate it world-wide? (Trends)**

Most experts say that the situation with the privacy and protection of personal data is at a positive trend in our country, and in the world. They think we cannot compare with the more developed western European countries, but that in our country, efforts are being made, and the awareness of this issue among the general public is slowly being raised. In that context, they noted the work of the Directorate for the Protection of Personal Data as a very positive trend, which is already producing results. All experts, including those who do not agree that there are positive trends in our country and the world, consider that in the developed democratic societies, there are very different conceptions of what privacy is, and the need of the right to privacy (including its protection) - and they split those in two "main" blocks - Western European countries, where the right to privacy is very respected and huge strides are being taken to protect the privacy and protect personal data, and the United States and Canada, where, there is virtually no right of privacy, i.e., where this right is being violated on a daily basis, and huge amounts of personal data, without the consent of citizens and consumers, is being exchanged, stored and processed.

...On one hand, we have no effective control of the state bodies – none whatsoever, of their processing of personal data. On the other hand, one way to improve this situation is with the so-called whistleblowing. The best cases in which abuse of personal data was revealed, are not the ones when an inspection came and caught someone, but the ones reported by people from the inside, as conscientious individuals...

Experts set our country - "in the middle", i.e., there is much room for improvement, especially on the awareness of the general population for this issue, but that in our country there are very positive examples as well, such as the adoption of the Law on Protection of Personal Data, the creation of the Directorate for the Protection of Personal Data, continuous revisions of internal rules for the operation of most state institutions to retain the proposed measures from the Directorate etc.

In addition, the views and opinions of the experts were noted before the interviews by using a simple survey. The answers of the experts are visually represented on the following pages.

The survey questionnaire filled out by all the participants before the interviews is provided below as an appendix, at the end of this publication.

> *"I think that awareness about privacy still doesn't exist, because the meaning of privacy is not defined among ordinary people."*

Expert's survey results:

An expert (representative) from each sector participated in the survey. We had two experts from the education sector. The remaining participants were from the following sectors: nongovernmental organizations, media, labor relations, public enterprises, telecommunications and insurance.

For the first question, experts made a division according to the laws in which certain sectors operate. Half of them had no answer to the question – "Based on which law is the collection of personal data envisaged for your sector?" The laws that they were able to identify were the Law on Higher, Secondary and Elementary education, as well as the Law on Insurance Supervision.

With the exception of two of the interviewed participants, the other participants were familiarized with the forms of personal data storage envisaged in the sectors.

With the exception of one participant, who stated that the purpose of collection cannot be clearly determined in the text of the laws, the other participants confirmed that the purpose of collection can be clearly determined in the text of the laws.

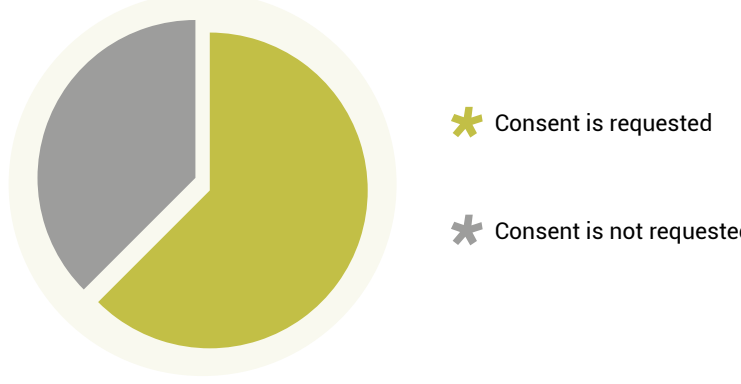
The position of the experts regarding the justification of the scope of personal data collection was that the scope is appropriate, i.e. 6 out of 8 respondents confirmed that the scope corresponds to the purpose.

With an exception of one of the interviewed participants, who stated that other state institutions are responsible for the collection of data in his sector, the remaining sectors have the capacity and stipulated legal obligations to collect personal data.

Half of the experts stated that they provide their data for use in accordance with the law, and the other half stated that personal data is not provided for use by third parties.

Most of the sectors (5 out of 8) envisage a request for consent from the data holder for the processing of his/her personal data, but only for specific personal data categories (see the graph above).

Graph 1: Consent for processing



Respondents cited the following as the most common purposes and categories for requiring consent: Personal Identification Number, name and surname, date of birth, phone number, medical records, address, bank account, and according to them - the most common reason for requiring consent was marketing purposes.

Half of the respondents stated that there are no clear and specific deadlines for personal data storage in the relevant laws, i.e. the text of the law does not stipulate it, whereas the other half claimed the opposite.

The question "How long can personal data be retained? – was answered by only three of the respondents: starting from 1 year, then 5 years, 10 years, and for an indefinite period of time (literature of permanent value), depending on the data.

Respondents were also divided when answering the question "Is there a separate article for personal data protection that clearly indicates the application of technical and organizational measuers? - 50% of them have applied technical and organizational measures, but half of the sectors have not applied the new technical and organizational measures for personal data protection.

With the exception of a respondent from one sector, the respondents from all other sectors responded that they have adopted additional internal acts in cooperation with the DPDP when asked "Has your sector adopted internal acts for technical and organizational measures for secrecy and protection of personal data?

"Is data processing stipulated in this law, or should it be related to and applied with another law?" – Two of the respondents stated that the processing of personal data is not stipulated in their law, so it is applied according to another law, while the other six respondents stated that the personal data processing is clearly indicated in the law itself.

When asked "Are there any exceptions for the processing of sensitive personal data (Personal Identification Number, biometrics, video surveillance) half of the respondents replied that there are such exceptions, and three respondents stated that these kinds of procedures are not applied in their sectors, i.e. there are no categories of personal data that are not processed (see the graph above).

Graph 2: Exceptions in processing

Out of the sectors that make exceptions and categorize personal data according to sensitivity, only a few are familiarized with the defined exceptions, i.e. 3 out of 8 cited the following categories of personal data that is not being processed: Personal Identification Number, medical records, video surveillance, and a representative of one of the sectors stated that they have a special database and registry of sensitive data, separate from the regular database.

Half of the sectors had no information about the availability of DPDP's opinions, whereas two of the respondents had information that the DPDP has not provided an opinion on those laws, and additionally only two of the respondents had information that DPDP's opinion has been taken into consideration for their laws.

PERSONAL DATA PROTECTION

Personal data protection is a relatively new legal concept in the Republic of Macedonia, although it is guaranteed by the 1991 Constitution. The right to protection of personal data is one of the fundamental human rights, but it is still debatable how much we know about it and whether we are able to recognize when our privacy is threatened?

The perception of people about what actually privacy means is different, but it is common to us that we are all aware of the need for protection of our privacy.

Personal data protection enters all segments of societal action, and this indicates just how complex is the matter in question. The large amounts of data we find everyday in different places and for different purposes, are imposing many questions about what actually happens to our personal data.

Where should we provide our personal identification number and for what purpose? Should the employer keep a photocopy of our personal ID and may we be monitored on the job? How should a health institution protect our medical records from abuse? Is it okay for us to see our names on a list of tenants who haven't paid for the maintenance of the building? For how long should we fill out forms with our data in the banks? Should we provide a copy of our personal ID when exchanging 10 euros? What do the cameras placed on the crossroads film and who owns that footage and photos?

These are just some of the questions that we inevitably ask ourselves more and more often, but what are the answers?

According to the Law on personal data protection, our personal data must be processed fairly and in accordance with the law and to be adequate, relevant and not excessive in relation to the purposes for which they are collected and processed. Rights guaranteed by this law: the right to inform ourselves on the purpose for which a certain institution or company collects and processes our personal data, the right to access the personal data that the institution or company is processing for us, the right to request the correction or deletion of incorrect data, excessive amounts of data for which the deadline for retention has expired, the right to accept or not to accept direct marketing.

Of course, we all have the right to turn to any institution or company and inform ourselves on how they guarantee the secrecy and protection of our personal data.

LEGAL ANALYSIS OF THE LAWS

Legal analysis methodology

Four stages were specified as necessary for the preparation of the legal analysis for compliance of certain laws with the Law on Personal Data Protection:

1. Defining the areas of application of the Law on Personal Data Protection
2. Specifying the applicable laws in the defined areas
3. Establishing the research methodology
4. Analysis of the answers to the questions set out in the methodology

Defining the areas of application of the Law on Personal Data Protection

Дефинирањето на областите каде примената на Законот за заштита на The identification of areas in which the application of the Law on Personal Data Protection is of particular importance to citizens was based on an analysis of the frequently asked questions posed by citizens to the Directorate for Personal Data Protection (DPDP) in the period from June 2011 to September 2014. The analysis included the answers that citizens had received from the DPDP, as an indicator of the situation in each separate area.

After the analysis of the citizens' questions and the answers of the DPDP, the following 12 areas were defined for the analysis: insurance, telecommunications, judiciary and security, banking, healthcare, media, labor relations, education, housing, social issues and public enterprises.

Specifying the applicable laws in the defined areas

After defining the areas in which the application of the Law on Personal Data Protection is of particular importance to the citizens, the applicable laws for each of the defined areas were also identified. A total of 35 laws were identified, and a database of the texts of all these laws was created.

Establishing the research methodology

After the methodology for conducing the legal analysis was established, it was necessary to define the questions that the legal analysis was required to answer.

The principles of personal data protection were used as the basis for defining the questions for the analysis. According to these principles, personal data is to be processed justly and in accordance with the law, to be collected for specific, clear and legally stipulated purposes and to be processed in accordance with those purposes, as adequate, relevant and not excessive in relation to the purposes for which they are collected and processed, accurate, complete and,

where necessary, updated and stored in a form that allows the identification of the personal data holder, but no longer than the time necessary to meet the purposes for collecting the data.

Hence, 11 questions were defined, based on which the analysis of the 35 laws from the 12 areas was carried out.

1. Does the law require personal data collection and in what form (records, registry, database)?

2. What is the purpose of the personal data collection and is the purpose clear?

3. Does the volume of data being processed match the purpose?

4. Who is collecting the data initially (company, institution)?

5. Should the processing of a certain data category be conducted with the personal data holder's consent?

6. Is there a defined period of time for storing personal data?

7. Is there a specific article for personal data protection that clearly indicates the application of technical and organizational measures?

8. Is the processing of the data stipulated in this law related or should it be related to the application of some other law?

9. Are there any exceptions for processing sensitive personal data? (personal identification number, biometrics, video surveillance)

10. Has the DPDP provided its opinion on the Law?

11. Was the opinion of the DPDP taken into consideration?

Analysis of the answers to the questions set out in the methodology

This is how the results from the analysis of the answers to the questions in the methodology are presented:

1. The answers to the questions are presented as facts, e. a confirmation or negation of whether the principles of personal data protection have been respected and

2. An explanation about the legislation for personal data protection and guidelines and proposals for complete harmonization of the separate laws with the Law on Personal Data Protection.

The opinions of the Directorate for Personal Data Protection regarding the compliance of the laws with the Law on Personal Data Protection were not delivered before this website was finalized, so they were not included in the legal analysis.

Results from the legal analysis of the laws

Law	Arrangement of legal content	Aim	Scope	Consent	Keeping time	Technical and organisational measures	Related with other regulative	Exceptions
Title of the law and Official Gazette number (last change or modification)?	Does the Law envisage processing of personal data and in what type of Collection (Evidence, Register, Database)?	What is the purpose of collecting personal data and is that purpose clear?	Is the scope of data being processed in compliance with the purpose?	Is the Consent of the data subject for personal data protection envisaged by this law?	Is the keeping period of personal data clearly defined?	Does the law contain separate provision for personal data protection that clearly states the implementation of technical and organizational measures?	Is the processing of personal data prescribed by this law connected to implementation of another law?	Are there any exceptions for processing of sensitive data? (PIN, biometrics, video surveillance)
LAW ON INSURANCE SUPERVISION	✓	✓	✓	⊗	✓	✗	✓	✓
LAW ON COMPULSORY TRAFFIC INSURANCE	✓	✓	⊗	⊗	✓	✗	✓	✓
LAW ON PENSION AND DISABILITY INSURANCE	✓	✓	✓	✗	✓	✗	✓	✓
LAW ON HEALTH INSURANCE	✓	✓	✓	✗	✗	✓	✓	✓
LAW ON HEALTH RECORDS	✓	✓	✓	✓	✓	✓	✓	✓
LAW ON HEALTH PROTECTION	✓	✓	✓	✗	✓	✓	✓	✓
LAW ON PROTECTION OF PATIENTS RIGHTS	✓	✓	✓	✓	⊗	⊗	✓	✓
LAW ON TRAFFIC AND ROADS SAFETY	✓	✓	⊗	✗	⊗	✗	✓	✓
LAW ON SAFETY AND HEALTH AT WORK	✓	✓	✓	✗	✗	✗	✓	✓
LAW ON LABOR RELATIONS	✓	✓	✓	✗	✓	✓	✓	✓
LAW ON RECORDS IN THE FIELD OF LABOR	✓	✓	✓	⊗	✓	✓	✓	✓
LAW ON EMPLOYMENT AND INSURANCE AGAINST UNEMPLOYMENT	✓	✓	✓	✓	✓	✓	✓	✓
LAW ON COMPULSORY CAPITAL FINANCED INSURANCE	✓	✓	✓	✗	✓	✗	✓	✓
LAW ON CIVIL SERVANTS	✓	✗	✗	✗	✗	✗	✓	⊗
LAW ON PUBLIC SERVANTS	✓	✗	✗	✗	✗	✗	✓	⊗
LAW ON DWELLING	✓	✓	✓	✓	✓	✗	✓	✓
LAW ON REAL ESTATE CADASTRE	✓	✓	✓	✗	✗	✓	✓	✓
LAW ON RECORDS OF BIRTHS, DEATHS AND MARRIAGES	✓	✓	✓	✗	✗	✗	✓	✓

Law	Arrangement of legal content	Aim	Scope	Consent	Keeping time	Technical and organisational measures	Related with other regulative	Exceptions
Title of the law and Official Gazette number (last change or modification)?	Does the Law envisage processing of personal data and in what type of Collection (Evidence, Register, Database)?	What is the purpose of collecting personal data and is that purpose clear?	Is the scope of data being processed in compliance with the purpose?	Is the Consent of the data subject for personal data protection envisaged by this law?	Is the keeping period of personal data clearly defined?	Does the law contain separate provision for personal data protection that clearly states the implementation of technical and organizational measures?	Is the processing of personal data prescribed by this law connected to implementation of another law?	Are there any exceptions for processing of sensitive data? (PIN, biometrics, video surveillance)
LAW ON PRIMARY EDUCATION	✓	✓	✓	✗	✓	✓	✓	✓
LAW ON SECONDARY EDUCATION	✓	✓	✓	✗	✗	✗	✓	✓
LAW ON HIGHER EDUCATION	✓	✓	✓	✗	✓	✓	✓	✓
LAW ON ADULT EDUCATION	✓	✓	✗	✗	✗	✗	✗	✗
LAW ON PEDOPHILIA	✓	✓	✓	✗	✗	✗	✓	✓
LAW ON SOCIAL PROTECTION	✓	✓	✓	✗	✗	✓	✓	✓
LAW ON THE GAMES OF CHANCE AND ENTERTAINMENT GAMES	✓	✓	✓	✗	✗	✗	✓	✗
ENERGY LAW	✓	✓	✓	✗	✓	⊗	✓	✓
LAW FOR REGULATING THE PROCEDURE OF COURT TRIALS	✓	✓	✓	✗	✓	✓	✓	✓
LAW ON SECURING CLAIMS	✓	✓	✓	✗	✗	✓	✓	✓
LAW ON LITIGATION PROCEDURE	✓	✓	✓	✗	✓	✗	✗	✓
LAW ON PAYMENTS OPERATIONS	✓	✓	⊗	✗	✓	✗	✗	⊗
LAW ON MEDIA	✗	✗	✗	⊗	✗	⊗	✗	✗
LAW ON TAX PROCEDURE	✓	✓	✗	✗	✗	✓	✓	✓
LAW FOR PREVENTION OF MONEY LAUNDERING AND FINANCING OF TERRORISM	✓	✓	✓	✓	✓	✓	✓	✓
BANKING LAW	✓	✓	✗	✗	✗	⊗	✓	✓
LAW ON ELECTRONIC COMMUNICATIONS	✓	✓	✓	✓	✓	✓	✓	✓

✓ Completely fulfils the criteria of the analysis

✓ Generally, fulfils the criteria of the analysis, with some issues (see Law Recommendations)

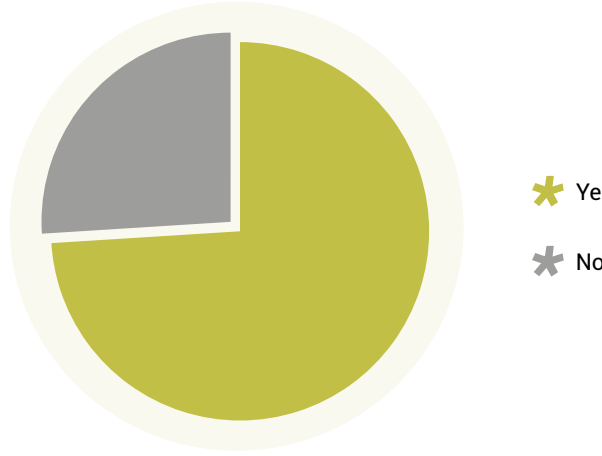
✗ Does not fulfil the criteria of the analysis

⊗ Does not fulfil the criteria of the analysis although some parts are covered

Graphic display of the results from the legal analysis of the 35 analyzed laws:

Volume

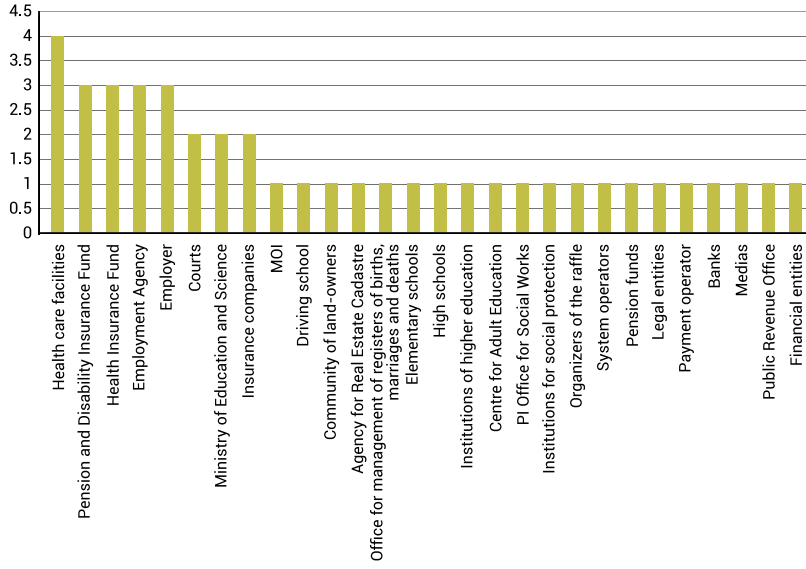
Does the volume of data being processed match the purpose?



The volume of collected personal data matches the purpose in most of the cases.

Controller

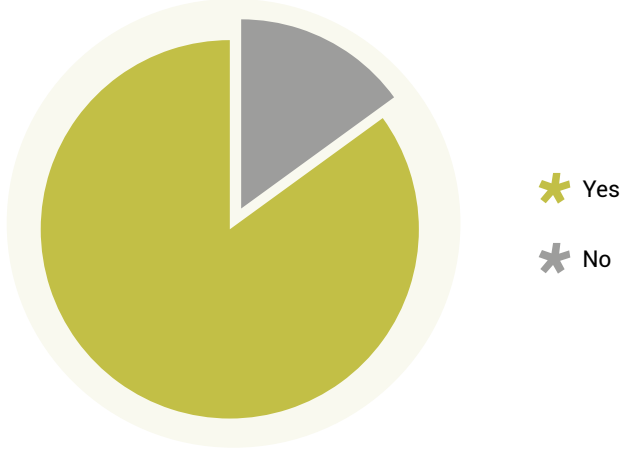
Who is collecting the data initially? (company, institution)



Often, controllers are health institutions, the Pension and Disability Insurance Fund, the Health Insurance Fund of Macedonia, the employer and the Employment Agency of the Republic of Macedonia.

Consent

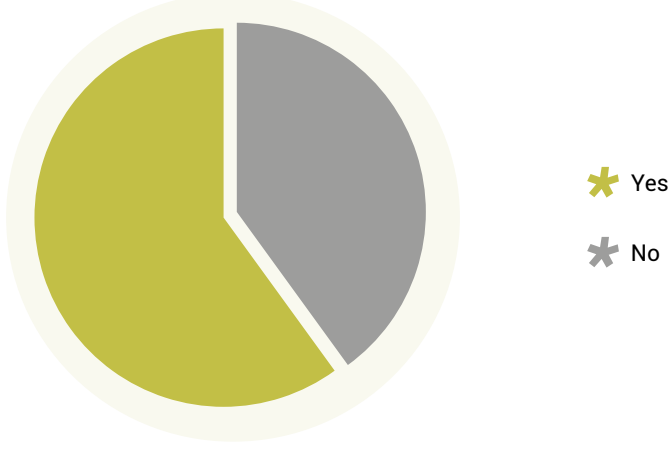
Should the processing of a certain data category be conducted with the personal data holder's consent



The request for consent from the data holders is stipulated in a small portion of the laws that were analyzed.

Technical and organizational measures

Is there a specific article for personal data protection that clearly indicates the application of technical and organizational measures?



This article is not implemented in more than half of the analyzed laws.

RECOMMENDATIONS FROM THE RESEARCH

Recommendations by areas

During the preparation of the legal analysis of the laws, we came across typical omissions in terms of personal data protection, according to the area of the particular laws. Aside from the recommendations for each of the laws that were analyzed, we are also providing the following recommendations by areas:

1. INSURANCE

Generally, in the insurance area it is necessary to precisely define the categories of collected personal data of the insured – from the introduction of the Personal Identification Number in the Law on Insurance Supervision – to the introduction of health personal data collected for the electronic health card in the Law on Health Insurance. The categories of personal data should also be precisely defined in the Law on Compulsory Traffic Insurance, in the Law on Pension and Disability Insurance and in the Law on Mandatory Fully Funded Pension Insurance.

The obligation for adopting laws and for applying technical and organizational measures for personal data protection in the laws in the insurance area is required not only for the internal regulation of the work of the controllers, but also for signing agreements with the users, for obtaining data from other entities and for recordkeeping about the data processing.

The periods for storage of personal data are not clearly defined for all types of recordkeeping in the laws related to the insurance area. Some of these laws stipulate "the shortest period for storage" which is not in accordance with the Law on Personal Data Protection, because the deadline should be precisely defined.

2. HEALTH PROTECTION

The analysis of the Law on recordkeeping in the area of health, the Law on Health Protection and the Law on Protection of Patients' Rights, indicates that the provisions in the area of health data recordkeeping, protection of patients' rights and personal data protection are applied for the recordkeeping, storage, collection and handling of the medical documentation. If we take into consideration how this provision is applied in practice, then every health institution needs to adopt and apply technical and organizational measures for secrecy and protection of personal data. The periods for storage of personal data stipulated in the laws related to health protection are not clearly defined for all types of recordkeeping. Deadlines for storage of personal data need to be specified.

3. LABOR RELATIONS

In accordance with the Law on Health and Safety at Work, the Law on Labor Relations, the Law on recordkeeping in the area of labor and the Law on employment and insurance in case of unemployment, the personal data that is being processed should correspond to the purpose for which they were originally collected. The categories of personal data are defined in detail for each record separately, however, practice shows that a photocopy of an ID card is being collected for more records than stipulated, although it is not envisaged with this law, and this is not in compliance with the principles of personal data protection.

Certain additions and adjustments should be made in the Law on Health and Safety at Work in the area of defining the method of delivery of reports from the health facilities to the employer. Practice shows that there are cases in which the general report is not separated from the results of the conducted examination.

As for the definition and application of technical and organizational measures for secrecy and protection of personal data, it is necessary to clearly establish responsibility of the employer for creating rulebooks for protection of the personal data of employees and personal data of other stakeholders.

Although some of the employees' contact details being collected may be entered optionally, such as, for example, the ethnicity of employees should be data that the employee chooses whether to provide or not, and the consent of the employee is not stipulated anywhere in the Law. The consent of the employees should be stipulated in the law.

The records for employees and records for wages are kept permanently, but other records containing personal data should be linked to the Law on filing.

4. HOUSING

The extent of personal data processed in accordance with the Housing Law is corresponding with the purpose, but practice shows that a high volume of data is being published on bulletin boards in the buildings – there is no provision in the Housing Law stipulating the publication of a list of tenants (their name and surname) who haven't paid for the maintenance of the building, and therefore this data processing is considered to be excessive in terms of the objective that should be achieved.

A period for storage of data is envisaged only for video surveillance – 30 days. It is necessary to also specify the periods for storage of other personal data.

Although harmonization with the Law on Personal Data Protection is projected, the law does not include an article stipulating an obligation of the community of tenants for interior regulation of the technical and organizational measures for personal data protection.

In terms of the Law on Real Estate Cadastre, it is necessary to precisely define the categories of data to be collected in the Geodetic-cadastre information system.

The deadlines for storage of the collected personal data must be clearly defined.

5. EDUCATION

In accordance with the Law on Primary Education, Law on Secondary Education, Law on Higher Education and the Law on Adult Education, consent from the personal data holders is not envisaged for personal data that is not listed in the categories of data – collected in practice, i.e. included in the (EMIS) software (health data, blood type, personal identification number of the parent). Consent for the processing of this data should be stipulated, as well as the software possibilities for the availability of this data.

The provision defining that the high school collects, processes, stores, sends and uses data included in the data sets in accordance with the regulations for personal data protection – for the integrated database maintained by the Ministry – is vague in the section pertaining to data sending. It should be defined where the data can be sent and under what conditions.

All the deadlines for storing personal data should be defined in all the specified laws and an article about the method of personal data protection should also be added, as stipulated in the Law on Primary Education.

The categories of personal data to be processed are not defined in the Law on Adult Education, although recordkeeping is stipulated. The article only stipulates that the content and form of the documentation and recordkeeping are regulated by the Minister, at the suggestion of the Center, which is not in accordance with the principles for personal data protection.

6. SOCIAL ISSUES

The analysis of the Law on a special registry for persons convicted for crimes of sexual abuse of minors and pedophilia, indicates that the purpose of processing personal data is to provide protection of children from sexual abuse, pedophilia and minors trafficking by providing information about the people who are convicted for such crimes and are living in their vicinity.

This is not in accordance with the principles for protection of personal data in terms of the availability of information. The practice in the countries that have such a registry is to limit the access to this registry, i.e. access to the registry is only granted to kindergartens, schools, orphanages and boarding schools.

The scope of the data included in the registry would be appropriate if access is restricted. In this case, when the register is publicly available, it's necessary to reduce the scope of personal data (initials, year of birth, residential address).

The exclusion from the public registry upon the request of an individual is contrary to the principles for personal data protection. The controller should exclude the data after the deadline expires, regardless of whether the individual requested it or not.

As for the Law on Social Protection, it is necessary to include an article stipulating the application of technical and organizational measures for secrecy and for protection of personal data, and it is also necessary to define the periods for storage of personal data collected for the purposes of this law.

7. GAMES OF CHANCE AND ENTERTAINMENT GAMES

The periods for storage of personal data should be defined for each record separately.

An article should be added, stipulating the application of technical and organizational measures for secrecy and for protection of personal data.

8. PUBLIC AND STATE INSTITUTIONS

In the Energy Law, it is necessary to define the obligations of operators for adopting rules for the application of technical and organizational measures for the secrecy and protection of the personal data of consumers.

A clarification is needed in the provision relating to the scope of personal data that is collected. The scope is appropriate, except in the section regarding the support with proof for personal identification. This formulation is ambiguous, and also leaves room for keeping photocopies of personal documents, which is not in accordance with the principles for personal data protection.

The periods for storage of personal data should be defined for each record separately.

An article should be added, stipulating the application of technical and organizational measures for secrecy and for protection of personal data.

The Law on Civil Servants stipulates a registry of civil servants to be created as a personal data set, but the personal data to be processed in this set are not defined, and neither is the method of processing. Also, no deadlines for data storage are provided and these two laws should be amended in accordance with all the principles for personal data protection.

9. MEDIA

The subject matter regulated by this law is specific in terms of the application of the principles for personal data protection, and it is not possible to precisely define all the data for persons included in media reports or persons connected to them. However, it is necessary to define precise guidelines for the publication of personal data of the persons included in the media reports. This would also set standards for the just processing of personal data, leading to the introduction of technical and organizational measures for protecting the personal data from the media. This law should also stipulate the consent of the data holder.

10. BANKING

It is necessary to amend the provision stipulating the following: the data is provided to the Ministry of Labour and Social Policy, the Employment Agency of the Republic of Macedonia and the Health Insurance Fund of Macedonia, for the purpose of performing their tasks and in accordance with the regulations for personal data protection, only if a bank signs a memorandum of cooperation with these institutions, regulating the method of availability of the data. First of all, the very approach is arguable as an activity, and second – the grounds for allowing it.

The stipulated signing of a memorandum for cooperation with the institutions in order to obtain data is arguable, as the memorandum does not have the legal power to allow this. It is not a document based on which those who are affected the most – the citizens, can exercise a right or be able to disagree. This puts into question the seriousness of the banks, particularly due to the fact that the bank secret is no longer a secret, because of the exception for revealing the secret to the institutions.

As for the regulation of payment transactions, in accordance with the law – the Minister of Finance regulates the payment instruments and their content and form, except the form of payment instruments included in the transfer media. With this kind of formulation, the content of the payment instruments is still to be determined with a rulebook, which is not in accordance with the principles for personal data protection.

Practice indicates that for payments from physical entities, the payment instrument contains a personal identification number, and there are no legal grounds for this.

11. JUDICIARY, ENFORCEMENT AND LITIGATION

The Civil Procedure Law contains a provision defining the scope of personal data. The scope is appropriate, except in the section regarding the support with proof for personal identification. This formulation is ambiguous, and also leaves room for keeping photocopies of personal documents, which is not in accordance with the principles for personal data protection.

An additional intervention is required in this law, in order to specify the periods for storage of personal data for each record separately, as well as the technical and organizational measures for secrecy and protection of personal data.

The scope of personal data stipulated in the Law on enforcement suits the purpose, with a remark that the scope of data for the persons for whom the enforcement agent makes a public announcement is not precisely defined. A citizen's personal identification number is often included in the announcement, and there are no legal grounds for this.

It is necessary to define the periods for storage of personal data for each record separately, and to add an article stipulating the application of technical and organizational measures for secrecy and for protection of personal data.

12. SECURITY

The categories of personal data processed in the records of the Law on Road Safety are defined in other laws and rulebooks of the Ministry of Interior. The scope of personal data needs to be completely regulated in the records with surveillance footage of the roads.

Since video surveillance is regulated by the Law on Personal Data Protection, it needs to be compliant with the principles for fair video surveillance. The goal is clear and justified, but it's necessary to specify the personal data that is to be collected (the focus of recording cameras), who from the police will have access to the recorded materials, how will they be sent to the driver or the vehicle owner. The law should also stipulate special alerts drivers for drivers at places where a video surveillance system is set up.

Periods for storage should be specified, except for the video surveillance footage, for which the projected period for storage is six months.

The Law does not include an article for personal data protection, hence the need to include a specific section about personal data protection, i.e. about the technical and organizational measures guaranteeing the secrecy and protection of the data.

PROCEDURES FOR REPORTING MISUSE OF PERSONAL DATA AND VIOLATION OF THE RIGHT TO PRIVACY

What should you do if you think your right to privacy or your personal data has been violated?

First, you can submit a request to the Directorate for Personal Data Protection (DPDP) - **Request for establishing a violation of the right to protection of personal data**. The Directorate can further contact you for handling the request.

If a company or institution has violated your privacy or misused your personal data, you can simply submit a free initiative requiring inspection to be performed by the Directorate, as follows:

Fill out the form - **Initiative for conducting inspection**. All you have to do is describe your problem.

1. In the form, first enter the title or the name and surname of the controller who misused your personal data or acted contrary to the Law on Personal Data Protection.

2. Then, briefly describe the violation and indicate what exactly have you done so far, and whether you have received a response from the controller for the specific case.

3. Please attach copies from the correspondence between you and the controller, as well as any other evidence, if available. If you plan to submit the form electronically, please scan and attach the copies.

The completed form can be submitted electronically to: **info@privacy.mk**

If you are not able to send the form via e-mail, print it and deliver it to the archive of the Directorate for Personal Data Protection or send it by regular mail to ul. Goce Delchev, no. 18, 1000 Skopje. (the Directorate for Personal Data Protection is located in the building of the Macedonian Radio and Television).

How long does the inspection procedure last?

The deadline for acting on the initiative is stipulated in the Law on Personal Data Protection. The inspector submits a report to the controller within 30 days of the completion of the inspection. The controller has the right to submit remarks on the report within three days. After these deadlines, the inspector submits a request for violation removal to the controller. The Directorate for Personal Data Protection will then notify the petitioner about the result from the procedure.

ANNEX

Annex 1.

Survey questionnaire for interview participants

1. Does the law you're working with stipulate personal data collection and in what form (records, registry, database)?

Law (please specify)_____

records registry database not stipulated

2. Is the purpose for personal data collection clear?

Yes No

3. Does the volume of data being processed match the purpose?

Yes No

4. Who is collecting the data initially? (name of company, institution)

_____

5. Does another personal data holder have the right to access this data, i.e. are you providing the data for use or processing by another institution or company?

Yes No

6. Is the processing of a certain data category conducted with the personal data holder's consent? If so, what category?

Category/categories:_____

Consent is not stipulated

7. Does the law you're working with stipulate a clear and specific period of time for storing personal data?

Yes How many years or months?_____

No

8. Is there a specific article for personal data protection that clearly indicates the application of technical and organizational measures?

Yes No

9. Have you adopted internal acts for technical and organizational measures for secrecy and protection of personal data?

Yes No

10. Is data processing stipulated in this law, or should it be related to and applied with another law?

This law Another law

11. Are there any exceptions for processing sensitive personal data? (personal identification number, biometrics, video surveillance)

    Yes Example_____ No exceptions

12. Has the DPDP provided an opinion on the law and was this opinion taken into consideration?

    Yes, and it was taken into consideration

    Yes, but it was not taken into consideration

    No

Annex 2.
List of the analyzed laws (alphabetical order)

Consolidated versions of all the analyzed laws - applicable at the time when the analysis was created, are available in the "Библиотека" (Library) section of the "Приватност" (Privacy) website **http://privatnost.mk/biblioteka-na-zakoni/.**

Banking law
Energy law
Law for prevention of money laundering and financing of terrorism
Law for regulating the procedure of court trials
Law on adult education
Law on civil servants
Law on civil servants
Law on compulsory capital financed pension insurance
Law on compulsory traffic insurance
Law on electronic communications
Law on employment and insurance in case of unemployment
Law on enforcement
Law on games of chance and entertainment games
Law on health insurance
Law on health protection
Law on health records
Law on higher education
Law on housing
Law on insurance supervision
Law on labor records
Law on labor relations
Law on litigation procedure
Law on media
Law on payments operations
Law on pedophilia
Law on pension and disability insurance
Law on primary education
Law on protection of patients' rights
Law on real estate cadastre
Law on records of births, deaths and marriages
Law on secondary education
Law on social protection
Law on tax procedure
Road traffic safety law
Work health and safety law

Bibliography

Council of Europe, Office of Treaties, **http://conventions.coe.int/**

Electronic Privacy International Center (EPIC), **www.epic.org**

EPIC, (2004), Privacy & Human Rights – An International Survey of Privacy Laws and Developments, United States of America

EPIC, (2006), Privacy & Human Rights – An International Survey Of Privacy Laws And Developments, United States of America

Privacy International, EPIC, CMCS, (2010), European Privacy and Human Rights (EPHR) 2010, **http://goo.gl/xzHv80**

Akademika, Electronic collection of Macedonian regulations in force, **https://www.akademika.com.mk/**

Directorate for Personal Data Protection, **www.dzlp.mk**

European Digital Rights, **https://edri.org/theme/privacy/**

European Data Protection Supervisor, **edps.europa.eu**

Kenig, Nikolina, (2008), Qualitative Research Methods, Faculty of Philosophy, Skopje

Comment on the Law on Personal Data Protection, (2010), Directorate for Personal Data Protection, Skopje

Mini-survey about children's internet habits, (2011), Metamorphosis Foundation, Skopje, **http://goo.gl/jbA5rj**

Neuvirt, Karel, (2007), Privacy as a fundamental human right, Metamorphosis Foundation, Skopje, **http://goo.gl/dmfHsb**

Pravdiko, website for education in the area of law, **www.pravdiko.mk**

Constitution of the Republic of Macedonia, **http://www.sobranie.mk/ustav-na-rm.nspx**

METAMORPHOSIS