Dear readers,

It is our honor and pleasure to introduce you with the sixth edition of the e-newsletter of the Directorate for Personal Data Protection.

The first half of this year was fulfilled with numerous activities and organization of events on international level.

This time allow me to briefly inform you about our activities and initiatives constantly trying to promote the right of protection of personal data and the right of citizens.

In this regard was the organization of two international conferences with numerous participants and experience exchange, opinions and concerns, in reference to the issues and topics that mark the newest proposals of EU data protection reform package.

Setting up new mechanisms for informing, raising public awareness for abuse of personal data, abuse of secrecy of correspondence, privacy issues of concerns, are only topics and issues which are imposed by our citizens as well.

Our aim is not only to react duly on time to all requests for establishing the right to protection of personal data and the right to privacy, but to react in preventive way with the aim of prevention of risks and creation of modern society rich with culture of data protection knowledge and respect towards privacy policies exists.

Dear readers,

In order for continuing introduction to various topics relating to your right to protection of personal data and privacy, we are deeply convinced that you will find interesting information in this edition of the e-newspaper.

Respectfully,

Director

Dimitar Gjeorgjievski

“i own my privacy”
DPDP
The 16th Meeting of the Central and Eastern Europe Data Protection Authorities – CEEDPA was organized in Skopje, the Republic of Macedonia in the period of 02-03 of April, 2014, whereas DPDP was a host.

Representatives from Data Protection Authorities from Central and Eastern Europe, i.e. Albania, Bulgaria, Czech Republic, Montenegro, Macedonia, Hungary, Serbia, Poland, Romania, Slovakia, Slovenia, Bosnia and Herzegovina, Georgia, Moldova and representative from the Council of EU, were gathered in Skopje to discuss for many issues of concern, as well as for the results achieved in 2013. During the two working days it was discussed the modernization of the legislation for personal data protection, “big data” challenges, smart metering, video surveillance of employees, protection of personal data in election processes.

In reference to the modernization and amendments on the Law on personal data protection, representatives of the Republic of Macedonia introduced the newest proposals of having third party as data protection surveillance mechanism, special attention for the area of anonymization of courts decisions, analyses of lawsuits, mostly experiences exchanged and lessons learned from all of the participants. Also, video surveillance on private property did raise some questions. Video surveillance for employee control modalities were discussed as well, particularly from the aspect of the protection employer’s legitimate interest and the protection of the right to dignity of employees. two declarations were adopted and signed:

A Declaration on new member of CEEDPA – as of second of April, Georgian DPA is a new member to CEEDPA, which resulted by great support from all members, showing that benefits from CEEDPA enlargement are significantly more valuable when we share experiences, and

A Declaration on mutual assistance and enhanced cooperation;

The second Declaration was in light of expressing the joint need for strengthening our cooperation and marking the current state of works on change of the EU data protection framework, and as a host, Macedonia strongly considered as important to establish a firm voice to be heard from the Central and Eastern Europe on urging EU Council for prompt adoption of future EU data protection regulation. especially taking into account the ongoing works on the ‘one-stop-shop’ system within the future EU data protection framework, which provides for specific competences and scope of responsibilities of DPAs in the context of trans-border data processing, under that provision of circumstances this should be considered as a step forward from the countries of Central and Eastern Europe, and among them the non EU member states, to declare and adopt such narrative.

One must admit that any declaration expressing support to each other, that brings down positive thinking and commitment towards collaboration are more than welcomed.

In that sense, a declaration on mutual assistance in situations arising from future EU data protection package and recalling for the Council of Europe and the European Union to guarantee consistent framework, as well supporting activities for building capacities of DPA in non-EU members are issues of necessity, and as a fact were recognized and adopted by all CEEDPA members.
You are Safe!

Campaign for the Protection of Personal Data in the insurance sector

The Directorate for Personal Data Protection in partnership with 13 companies and two insurance brokerages, and supported by the National Insurance Bureau and the Agency for Insurance Supervision, on 05.16.2014, starts the campaign - YOU ARE SAFE!

The insurance sector is a specific sector which manages insurance, which means, conclusion and execution of contracts for life insurance and non-life insurance. As long as insurance companies, insurance brokerages, insurance agents and companies that represent insurance, are responsible for the processing of personal data of insurers, they must provide accurate and complete information and to be informed about their obligations and rights under the laws and contracts concluded with these insurance entities.

In order to raise awareness of insurers for the protection level of the processing of their personal data by all stakeholders in the insurance sector in order to increase the scope of the insured citizens, as in life and non-life insurance in the Republic of Macedonia, for their obligations to provide personal data in the context of the exceptions to the application of the Law on Protection of Personal data, five open days will be organized, where citizens can be informed of whether insurance companies, insurance brokerages, insurance agents and companies that represent insurance, are entitled to process our ID number, to retain a photocopy of identity card or passport, to disclose personal data to third parties, carry out direct marketing for new products, services, contests and which are the rights and obligations of citizens for protection of their personal data when agreement for non-life insurance or life insurance is concluded.


May 16, Skopje City Mall
12:00 to 16:00 pm

May 20, Gostivar, City Square
10:00 to 14:00 pm

May 22, Stip, Vanco Prke
11:00 to 15:00 pm

May 26, Bitola, Magnolia Square
12:00 to 16:00 pm
Humanitarian action of DPD and the Red Cross of Macedonia

In anticipation of the Easter holidays, and in order to fulfill its human commitment for action and help to the poorest and most vulnerable, teams of the Directorate for Personal Data Protection and the Red Cross of the Republic of Macedonia Skopje visited three families to whom food and clothing were donated.

The Directorate for Personal Data Protection and the Red Cross of Republic of Macedonia for the second time organize joint charitable action, on the basis of the Memorandum of Cooperation signed with the Red Cross of the Republic of Macedonia in July 2012.

At the Book Fair—READ - and PROTECT YOUR PERSONAL DATA!

In light of the already established good cooperation with “Prosvetno delo”, and in the spirit of achieving joint activities, the Directorate for Personal Data Protection, with its promo desk- is present at the Book Fair, at the desk of the biggest publisher “Prosvetno delo” from the period of 8 to 14 of April, 2014.

The purpose of the presence of representatives of the Directorate for Personal Data Protection is a direct and immediate education for the right to protection of personal data, as well as completing several questionnaires designed especially for children and parents, in order to analyze the level of awareness and the level of knowledge of the subject to the privacy and protection of personal information, especially for the target groups in the educational process.

The analysis of the responses received to the questionnaire led to the following claims:

- 46 % of students say that while using social networks they consult the privacy policy, while 37 % do so only sometimes
- 83 % of parents believe that children should take care of their personal data
- Social networks are most fearful for the parents, and 68% of them believe that this is the biggest threat
- 76 % of parents believe that children are insufficiently educated in their school
- 60 % of parents would have addressed the Directorate if confronted with abuse.
TRAINING in the DPDP

The protection of personal data is an area that is constantly progressing, builds and monitors development trends of technology.

Continuing education for the implementation of the personal data protection principles is one of the ways to familiarize controllers with the legislation in this area.

Trainings on secrecy and protection of the processing of personal data are carried out by predetermined modules: one general and 16 specialized modules depending on the area controllers and processors are work related.

Information on Training Program for provision of secrecy and protection of the processing of personal data and Request for applications for training can be found at the following link.
BIG DATA—BIG problem!

By: Liljana Pecova Ilieska, M.A.

55-th meeting of IWGDPT and 2-nd Workshop on PHAEDRA Consortium

The Directorate for Personal Data Protection of the Republic of Macedonia with the Berlin Commissioner for Personal Data Protection was a host to the 55-th annual meeting of the International Working Group on the protection of personal data in the telecommunications sector, which was held on 05-06 May 2014 in Skopje. Experiences of international experts from member states of the European Union were shared and exchanged at this meeting, in special regard to BIG DATA and privacy as to the working document titled as: “Privacy principles under pressure in the age of BIG DATA analytics”.

Big Data is a term which refers to the enormous increase in access to and automated use of information. It refers to the gigantic amounts of digital data controlled by companies, authorities and other large organisations which are subjected to extensive analysis based on use of algorithms. Data is omnipresent. The amount of data on the global level is growing by 50 per cent annually. 90% of the world’s data has been generated within the past two years alone. Most of this data is generated by consumers through interaction with Internet-based services. Due to the proliferation of the Internet of Things, new data streams will be added. Countless sensors will upload information to cloud computing services on how humans interact with the things surrounding us. This may bring about a change in markets and business models.

It is estimated that there will be more than 50 billion sensors by 2015. In this context, information collected for web users is quite attracting for having the opportunity to get detailed information about the interests, habits, behaviors of individuals, activities, etc. What most concerns regarding the protection of privacy issues is that:

- Re-use the data for other purposes (data collected can be used for purposes not compatible with the original purpose for which they were collected)
- Maximization of data (the value of personal data contained in themselves)
- Compilation of data that can lead to disclosure of sensitive information (compilation of collected pieces of information can generate a sensitive data) controllers in particular should be aware of the risk in the compilation and analysis of data.
- Risk of re-identification - set of data can be set up for possible re-identification of persons, which may be anonymous; etc.

Most important of all is still adhering to the key principles of privacy protection: increased transparency, inform everyone individually about what and how data is collected about him/her, as well as the authority where may report, whether it will be performed transfer to third parties, if and where you can make anonymization, etc.
April 14 2014 (Monday) at the premises of MARRI - Regional Initiative on Migration, Asylum and Refugees, a memorandum of cooperation was signed between the Directorate for Personal Data Protection and MARRI. It is with the aim of implementation of joint activities, opening opportunities for education and information. Both directors expressed satisfaction that with the signing of this memorandum, not only declarative commitments are pointed out, but fields of work and contribution at the institutional and regional levels are opened. Mr. Trpe Stojanovski, Director of MARRI Regional Centre said: "We believe that we share the same goals and I believe we will have a smooth development of activities of particular interest in the upcoming period having in mind that R. Macedonia takes over presidency of MARRI." The Director of the Directorate for Personal Data Protection, Mr. Dimitar Georgievski said: "The protection of personal data is certainly important issue which is supposed to ensure sustainability in our overall performance in the context of long-term education, promotion, information and cooperation in the region. In this regard, we express our readiness to cooperate in the preparation of the Presidency priorities in the area of personal data protection in the target groups of the areas you cover, considering that the protection of fundamental human rights are priorities of Republic of Macedonia and EU."

Supported by the Office for Technical Support—TAIEX—European Commission, May 29, 2014, a workshop on "Cloud computing" was organized.

The Directorate for Personal Data Protection organized a workshop aimed at sharing good practices in relation to the risks arising from the use of cloud computing and the ways to overcome these risks. Also, the best examples of the legal regulation of the relationship between providers of cloud computing services and their customers were presented, in terms of protection of personal data that is transmitted. Experts from the surveillance authorities for personal data protection, from Slovenia, Denmark, Spain and the UK shared their experiences regarding the above issues and setting the technical and organizational measures to protect personal data. Also, an overview was given on the opinions and guidelines for cloud computing provided by the 29th Working Group.

TAIEX-Expert Mission

In the period from 19-21 May at the premises of the Directorate for Personal Data Protection, an Expert Mission on training for personal data protection was held, with support of German and Polish experts, in order to strengthen the capacity of the Commission on conducting training within the Directorate.
Regional legislation, including European legislation, may provide answers, but in practice technology and globalization oblige us to create standards that ensure a satisfactory level of protection worldwide.

Data protection will always be a "work in progress" that must keep pace with the new trends that are taking place continuously in the digital environment.


Prof. Dr. Artemi Rallo
Constitutional Law Professor at Jaume I University (Spain) and Phaedra Project Partner
Former Director of the Data Protection Spanish Agency, Deputy Chair of the Article 29 Working Party and Chair of the Data Protection Latin America Network

If there is one sector in which the need for a quick legal response is particularly important, it is new technologies. In this digital environment we are not dealing with a revolution, but with a constant, rapid evolution. While technology has clear and obvious advantages, its widespread use also presents challenges. For this reason, we need to reflect on the challenges that we face, on which agents are involved and how we can protect privacy appropriately.

We can identify three challenges in this digital environment:

Firstly, the fast development of tools that allow mass use of information in a more perfect way and that offer a multitude of information-processing possibilities. This results in at least two knock-on effects: a) The possibility to store, process and transfer large quantities of information, which has contributed to the high economic value of these services. On the Internet, personal information is a leading source of wealth. The most obvious example of this can be seen in advertising being individually tailored according to our browsing habits - behavioural advertising. b) Omnipresence is another phenomenon in this field today, which can be seen the convergence of Internet services with mobile technology.

Another challenge that we face is the transnational nature of these services: Companies operate in dozens of countries with different legal frameworks. At the same time, data are no longer kept in a specific location, but are rather spread among hundreds of servers around the world, as is the case with cloud computing.

Finally, but no less importantly, the Internet gives everyone a presence and a voice. The digital world has changed the role of individuals. People have also taken on an active role, which poses a challenge to current privacy regulations. People express themselves in blogs, microblogging networks or they share their experiences on social networks.

All of these factors, together with the increasing complexity of society, technology and business structures, lead us to consider the nature of the roles and responsibilities of users, business and governments. The clearest example of the complexity in assigning responsibility can be found in online social networks. When publishing information on a social network, who is responsible?

The Article 29 Working Party has looked into this situation and come up with a series of criteria. A paradoxical situation arises in which an individual becomes both the active and passive subject, making decisions on the information they process. This means such a person may be considered the processing controller, in the terminology of data protection legislation, subject to the same obligations as controllers. It is important to clarify that data protection legislation excludes data processing carried out by people "carrying out exclusively personal or domestic activities".

The Article 29 Working Party has set out some situations in which processing by social network users may go above and beyond this domestic activity exception.

More on the following link
Could you please check and if possible deactivate this FB profile ... because it is fake and uses data, photos and pictures of my family and friends and writes insulting issues on my real profile account.

Dear Madam/Sir,

The Directorate for Personal Data Protection of Republic of Macedonia, acting upon your complaint for deleting the fake FB account, has addressed to the Administrative Team for Support of the social networks Facebook, asking for removal of the reported false FB account.

The institution has no back-up server. The application software for processing of personal data is installed on a PC that is managed by one of the employees, which in turn is connected to another computer managed by head-officer. Question: Can a safety backup be made each day on a removable medium USB, and whether it can be kept in a locked cupboard in the institution?

Dear Madam/Sir,

Please note that it is ok to make safety backup daily, but despite that, at the end of the working day a backup should be archived and at the end of the working week, as well as, at every last working day of the month, according to Article 21 and Article 31 of the Rulebook on technical and organizational measures to ensure confidentiality and protection of the personal data. Furthermore, we inform you that monthly versions of security copies should be stored in another remote location. The medium can be transferred away from business premises only if personal data is encrypted or protected by suitable methods to ensure that data will not be readable, but only the information system administrator can decrypt it, or a person authorized by him.

More detailed information on the procedure for electronic data exchange and protection, as well as proper application of the Rules and Regulations for the technical and organizational measures to ensure confidentiality and protection of personal data processing, you can receive by contacting the following telephone number: + 389 2 630 635.
In Macedonia—usage of photos without consent is illegal, so watch out!

A person from Veles, Macedonia, is found guilty and received a suspended sentence because used a friend’s photograph and attached to video clip to YouTube. It refers to the crime act—abuse of personal data.”

According to the indictment during the month of June last year, contrary to the conditions laid down by law, without the consent of the injured D. D, his friend processed and used her personal information.

It did so through the social network Facebook, he took photos of the person concerned used them in a video, using audio recording from a cell phone using the program Windows movie maker and made a video clip.

It was published on 26/06/2013 Internet service Youtube titled My Movie snas-kam!!! In Veles the Trial Court imposed a suspended alternative measure if next year do any crime will go prison for three months.

Search removal request under European Data Protection law—Way to go GOOGLE!

A recent ruling by the Court of Justice of the European Union found that certain users can ask search engines to remove results for queries that include their name where those results are inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes for which they were processed.

In implementing this decision, we will assess each individual request and attempt to balance the privacy rights of the individual with the public’s right to know and distribute information. When evaluating your request, we will look at whether the results include outdated information about you, as well as whether there’s a public interest in the information – for example, information about financial scams, professional malpractice, criminal convictions or public conduct of government officials.

If you have a removal request, please fill out the form below. Please note that this form is an initial effort. We look forward to working closely with data protection authorities and others over the coming months as we refine our approach.

More on the following link