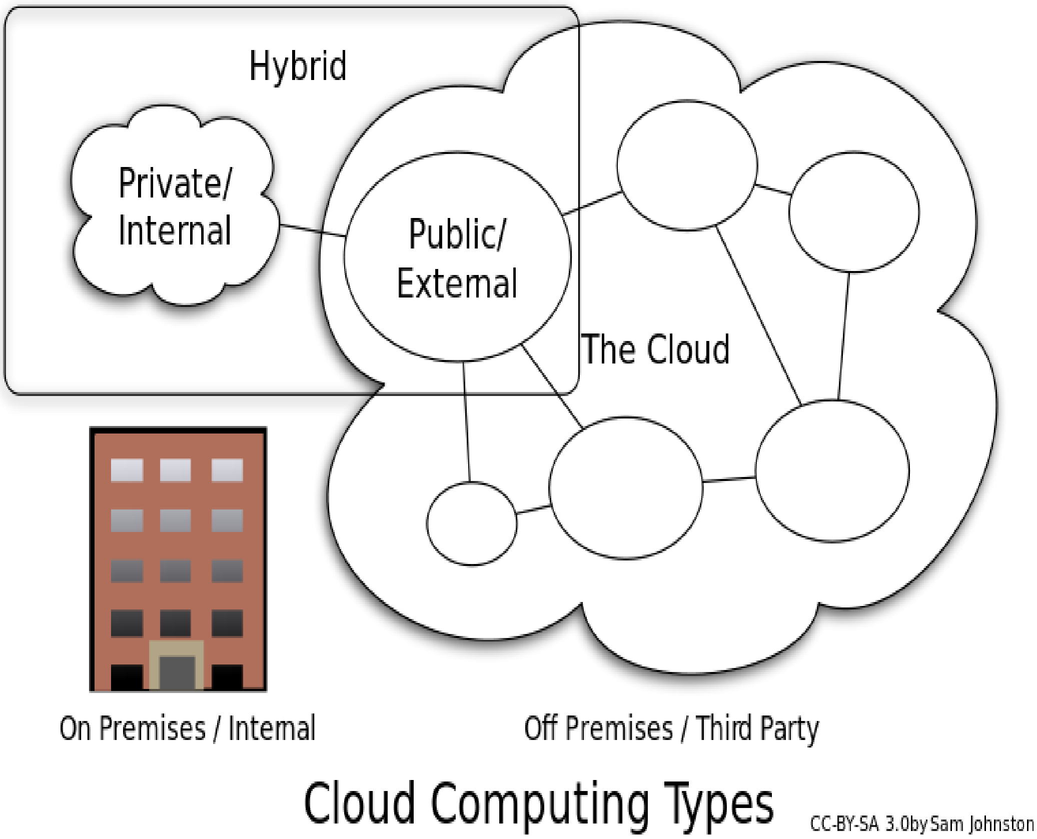
Analyses on current state of the organizational and institutional capacities for protection of personal data

"Technical Assistance for Enhancement of Organizational and Institutional Capacities for Personal Data Protection"

Directorate for Personal Data Protection

Skopje, February 2014



This analysis is part of the project entitled *"Technical Assistance for Enhancement of Organizational and Institutional Capacities for Personal Data Protection"*, which is carried out as part of the continuous development of the Directorate for Personal Data Protection of the RM.

The project is funded by the Ministry of Foreign Affairs of The Kingdome of Norway, as part of the bilateral cooperation between the Republic of Macedonia and the Kingdom of Norway.

Contents

I. INTRODUCTION AND GOALS

Recently (in the course of the past decade, in particular) we have been witnessing drastic development of the means of communication. Professional, as well as private communication is increasingly going on primarily online. Nowadays a good deal of data and information, as well as a great number of services and products, are available online. The main “culprit” for this situation is the internet. It is a powerful tool by which the service providers offer their services to the consumers.

However, online communication is two-way, which means that the service providers can also collect data and information related to the services users, i.e. the consumers, something that was utterly impossible and unimaginable in the times preceding this digital, information society. Thus, the service providers have identified in the internet a way how to increase their incomes, and the consumers, in turn, have welcomed the conveniences of purchasing online offered services, this leading to an increase both in the offer of online services and demand for them.

This process has been happening on a larger, countrywide scale. Countries and states have been offering their consumers online products and services, contributing thus to further development of the digital (information) society, but also cutting drastically down on the costs related to provision of these products and services. This also meant introduction of relatively new and previously unavailable services and products, due to the long distances, something which is now, with the internet, not an impediment at all.

Consequently, IT infrastructure required for provision of these online services has become of great significance, both for the providers of the services and for their users, i.e. the consumers, since both parties expect this infrastructure to be available and functional at any time and at any place, so that the data could be safely processed and stored.

Accordingly, one could draw a conclusion that development of digital society involves availability and development of a set of services available online through various media such as computers, mobile phones and the like.

Taking into account the above circumstances, this analysis strives to cast a light on the phenomena accompanying social networks and the concept of cloud computing, with respect to personal data protection, since this data does occur on the internet quite frequently and in more than one form. Personal data protection has become subject of intensive debates fostered by the drastic development of information technology (IT), the constantly growing number of products associated with data storage and processing, as well as their correlation. The debate in particular addresses the manner in which the products in question are being used.

This analysis is part of the project entitled *"Technical Assistance for Enhancement of Organizational and Institutional Capacities for Personal Data Protection",* which is carried out as part of the continuous development of the Directorate for Personal Data Protection of the RM. The project is funded by the Ministry of Foreign Affairs of The Kingdome of Norway, as part of the bilateral cooperation between the Republic of Macedonia and the Kingdom of Norway. This project aims at *further enhancement of organizational and institutional capacities of the Directorate for Personal Data Protection, in order to protect better and more efficiently the right of the individual's privacy on social networks, to improve the services offered by social networks related to privacy protection, to raise public awareness of the right of privacy protection when using the internet, and to improve public knowledge of modern technologies and issues related to privacy protection such as cloud computing.*

II. DIRECTORATE FOR PERSONAL DATA PROTECTION OF THE RM

The Directorate for Personal Data Protection (hereinafter referred to as: the Directorate) is an independent institution which is in charge of supervising the legitimacy of the activities related to processing personal data and its protection, on the territory of the Republic of Macedonia[1].

[1] It was established in accordance with the Law on Personal Data Protection ("Official Gazette of the Republic of Macedonia" No. 7/05, 103/08, 124/10, 135/11), and the Director of the Directorate is appointed by the Assembly of the RM. Accordingly, the institution is independent with respect to the executive, legislative and judicial authorities, as well as to the local authorities.

Every year the Director of the Directorate submits annual Report to the Assembly regarding the work performance of the Directorate. If needed and if requested by the Assembly, the Director of the Directorate submits an additional Report to the Assembly.

The report contains data related to the competencies of the Directorate[2] regarding preparation of legal decisions, texts and by-laws, development of policies associated with personal data protection[3], inspection supervision, assessment of the legitimacy of processing (supervision) of personal data, keeps a Central Register of sets of personal data and previously issued approvals for personal data processing, declares a ban on further personal data processing for those controllers who have not respected the regulations from the Law on Personal Data Protection, issues an approval for a cross-border transfer of personal data, runs infringement procedures[4] for infringements regulated by the Law, etc. The Directorate is also in charge of matters related to personal data protection of various supervisory authorities from other countries, when these matters are associated with the respective supervisory authorities' performing their activities in the Republic of Macedonia.

The Directorate is run by the Director. The Director is appointed and dismissed by the Assembly of the Republic of Macedonia, in a procedure led by a Commission for appointing officials by the Assembly of the Republic of Macedonia, by previously published public announcement for open vacancy, for a 5-year term and right to be reappointed, but not more than twice. The Director has a Deputy Director who gets appointed and dismissed by the Assembly, in a procedure led by a Commission for appointing officials by the Assembly of the Republic of Macedonia, by previously published public announcement for open vacancy, for a 5-year term. For their The Director and the Deputy Director are accountable

[2] The Directorate is not in charge of paying off monetary compensation for any kind of violation of the Law on Personal Data Protection; it does not keep personal data; can not prevent processing of personal data performed by a physical entity, provided it is done for his/her personal activities only or involves activities done within the home only; the Directorate is not in charge of processing personal data collected for the sake of protection of safety, security and defense of the Republic of Macedonia; it is not in charge of carrying out any kind of criminal procedures.

[3] Including international cooperation in the field of personal data protection and participation in the work of international organizations and institutions dealing with personal data protection.

[4] Through the Commission for handling infringements, in compliance with the law.

for their work before the Assembly. The Director manages the Directorate's administration which is organized into sectors and departments[5].

The Directorate's operation related to its "major" activities is being carried out through three sectors: Sector for Inspection Supervision, Sector for General and Legal Issues and Sector for European Integration, Projects and International Cooperation. Issues related to personal data protection on social networks and *"Cloud computing"* are handled by the Sector for Inspection Supervision and the Sector for General and Legal Issues.

The Sector for Inspection Supervision, through complaints and/or ex officio, with on-the-spot visits to the personal data controllers[6], supervises implementation of the measures related to personal data protection. It is this Sector where the inspectors (the Directorate) come into direct contact with the controllers who either use or provide services in a "cloud". The inspectors perform regular (yearly and monthly) supervisions, special supervisions and control supervision. The inspectors act pursuant to somebody's request/complaint or *ex officio*.

The Sector for General and Legal Issues in its Division for Normative-Legal Issues and for Handling Proposals and Charges deals with cases regarding privacy on social networks. The procedure regarding cases related to privacy infringement on social networks runs as follows: The Directorate receives complaints submitted in writing or in electronic form. The communication with the parties (the injured party - the stakeholders - the social network - the Directorate) runs both by face-to-face contacts and by electronic way. This procedure is pretty flexible and not that formal compared to the inspection supervision procedure. However, the increased activities of the Directorate and the growing number of complaints related to this issue (*see Chapter VI point 1 from this Analysis)* is likely to necessitate in future increment of the personnel dealing with this sort of cases (either by taking on new staff or by seconding of the existing employees, by appointing assistants and the like).

[5] (Annex 1 – organizational chart of the DPDP, source http://dzlp.mk/sites/default/files/Dokumenti/Organogram/ORGANOGRAM DZLP. pdf)

[6] If needed, to the data processors, too.

The Directorate also runs international cooperation, doing that in a few ways. The Directorate is a an equal voting member of the Consulting Committee (T-PD) of the Council of Europe of the Convention for Individuals' Protection against automatic processing of personal data, the European Conference for Personal Data Protection (Spring Conference), the Conference of Central and Eastern Europe Authorities for Personal Data Protection, the Working Group for Police and Judiciary, the International Conference of the Commissioners for Private Data and Privacy Protection, the International Working Group for protection of personal data in the field of telecommunications, case handling workshops etc. The Directorate also holds the status of an Observer in the Working Group 29 of the European Union.

In addition, the Directorate has also signed bilateral Declarations on Cooperation with 14 countries, predominantly from Europe and the region.

III. CONTEXT OF THE REPORT

1. Statistical Data[7]

As per the State Statistical Office, the number of internet users in Macedonia among households/citizens, businesses and public sector has been steadily growing since 2006, when statistical surveys in the filed of Information society[8] started to be conducted.

In 2006, 14% of the households/citizens had internet access from their homes[9], whereas in 2013 such was the case with 65,1%[10]. Out of the total number of those accessing the internet, 80,3% do that on a daily basis, and 92,7% do that from their homes. Out of the huge variety of reasons *(sending/receiving electronic mail - e-mail;* ***Participation in social networks;*** *reading on-line news/newspapers/magazines; searching for health-related information; searching for information related to education, training and courses; looking*

[7] Provided by the State Office for Statistics of the Republic of Macedonia.

[8] The surveys are conducted as per the methodology and recommendations of Eurostat (Statistical Bureau of the European Union), in compliance with the regulations of the European Union, i.e. the Regulation of the European Assembly number 808/2004).

[9] http://www.stat.gov.mk/pdf/2006/8.1.6.14.pdf, last time visited in November 2013.

[10] http://www.stat.gov.mk/pdf/2013/8.1.13.28.pdf, last time visited in November 2013.

for products/services-related information; downloading software (excluding games software); learning - attending online courses; learning - consulting online encyclopedia; looking for a job or sending job applications; participation at networks for professionals; using services associated with traveling and accommodation; sales of products/services (for instance, by auctions); telephoning via the internet / video calls by means of webcam; internet banking) for which individuals access the internet, most of the respondents, 84%, access the social networks, 69,6% of the respondents send/receive e-mails, and 61% use practice internet telephoning or video phoning. Only 5,6% of the respondents use the internet from home to participate in professional networks, and only 9,1% use the internet from home for internet banking[11].

In 2006, 72,3% of the legal entities with 10 or more employees[12] had access to internet, whereas in January 2013, broadband access to internet (by means of fixed or mobile connection) was available to 91,5% of legal entities with staff of 10 or more[13]. An exception to this figure are the legal entities from the financial sector, where as early as in 2006 100% of the staff had been using computers and the internet[14]. In 2013 7,4% of the legal entities had provided their staff with remote access to e-mail, papers and applications related to their company.

In 2013[15], for the first time there was a survey regarding usage of **social media** by legal entities, such as social networks, blogs, web sites for sharing multi-media information (e.g. Facebook, Twitter, You Tube etc) or wiki-tools for sharing knowledge. A figure of 36,2% of the legal entities [16] used the social media.

Concerning public sector, in the year 2006 access to the internet was available for 100% of the Ministries, 95,6% of the State Agencies/Organizations, 94,4% of Public Enterprises and

[11] http://www.stat.gov.mk/pdf/2013/8.1.13.28.pdf , last time visited in November 2013.

[12] This category of legal entities, as per the methodology of Eurostat, is considered relevant for comparison of data among the EU member states. According to Eurostat methodology, there are 4 categories of legal entities, out of which the second one is considered referential category.

[13] http://www.stat.gov.mk/pdf/2013/8.1.13.25.pdf , last time visited in November 2013.

[14] http://www.stat.gov.mk/pdf/2007/8.1.7.06.pdf , last time visited in November 2013.

[15] This data in fact refers to the year 2012, but it was processed and published in the report for 2013.

[16] http://www.stat.gov.mk/pdf/2013/8.1.13.25.pdf , last time visited in November 2013.

95,2% of the Local Authorities[17]. For legal entities in the public sector there are no surveys on usage of social networks or *"Cloud computing",* even though there are designed services that happen online on the web sites of the relevant institutions from the public sector, and these services are being offered to the citizens, legal entities and related institutions from the public sector.

No surveys have been conducted regarding application of *"Cloud computing"* as an independent item, owing to which it is impossible to get a clear idea of the extent of usage of these services in any of the sectors (households, businesses and public sector).

2. Social networks

Social networks on the internet, or usage of network services for linking and socializing with people who share common interests and activities, can be an excellent way of accomplishing specific interests, making new friends and improving the existing friendships, of playing games, exchanging ideas etc.

A few categories of web sites - social networks - have been identified.

Social networks of general character[18] -are services for general networking which can be joined by anyone and where people normally give their real identity. Accordingly, the site is primarily used for interaction with other individuals through the profile pages on the internet.

Business social networks[19] which differ from those with general character by the fact that the latter are specialized for professional contacts and for seeking job. Here the users commonly provide more professional than personal data, although the latter is not excluded.

[17] http://www.stat.gov.mk/pdf/2007/8.1.7.07.pdf , last time visited in November 2013.

[18] Windows Live Spaces, Facebook 5, MySpace, hi5, SkyRock, Friendster, NetLog, Tagged, Orkut, LiveJournal, Bebo, PerfSpot, meinVZ, Multiply, Badoo, Sonico, Ning, CyWorld, Plaxo
Bahu, Nexopia.

[19] LinkedIn, Viadeo and XING.

Social networks recommending a variety of film and music contents[20]. These sites normally contain some features similar to those of the sites of general character, but the users most commonly communicate among each other because they share common interests, types of music or films, rather than because of some real-world bonds.

Reunion sites[21] which allow for looking for old friends from, for instance, school or the army. The profiles on these sites are generally not maintained actively and only contact information is available. Yet, personal information can be provided.

Social networks for games[22], which enable their users to do some specific activities. Some of these activities may be playing games, obtaining information on traveling and the like. *Twitter* could be classified into this group.

Social networks – *sites with special privacy features*[23]. Here users can exchange experiences using pseudonyms, there are social networks for children with special parental care and administration of profiles and the like.

But, what is a social network? How does development of social networks affect privacy?

A social network is a form of interaction, when people first make contact with their acquaintances, and then virtually realize contacts with new individuals, with the purpose of accomplishing some private or business goals. Social networks enable their users to communicate without having a physical contact. The extent to which the communication will develop depends largely on the scope of data the users reveal about themselves. When creating the profile (user's account), the user is supposed to give information about oneself, data which may be not only personal but confidential, too. Despite the fact that most social networks leave it to the user to decide for himself which and how much personal information will give, which means that the user directly decides on the level of safety on that specific social network, quite often the users of the social networks do not think

[20] Last.fm, Imeem, Flickster, and Buzznet.

[21] Classmates.com and myLife (former Reunion.com)

[22] Habbo, Gaia Online, CouchSurfing.

[23] Kaioo, Experience Project, Imbee

enough or even not at all about this aspect of communication, thus putting themselves in danger.

Certainly, we must not forget the fact that users' profiles are created by legal entities too, most frequently for marketing and advertising purposes, which increases the value of a specific social network. The more users frequent a network, the higher its value gets. On the other hand, by analyzing the personal data provided by the users, the companies target those users who, according to the survey results[24], would be interested in the product or service advertised by the respective company, and who live in the vicinity of the place where that product or service is being advertised[25]. This fact must be taken into consideration when talking about privacy and personal data protection, as well as the risks related to this sphere, described below.

Personal data protection is particularly difficult to carry out in cases of social networks, since the personal data is provided by the users themselves. Thus, the potential risks for good-quality personal data protection include:

- Cases of *phishing u pharming*. Both activities are quite frequent and are being practiced by cyber-criminals, whose intention is to gather personal or financial data about the internet users (credit cards, PIN codes etc.)
- *Spam on social networks.* Usage of social networks as a platform for sending undesired messages.
- *Unauthorized indexing* by the internet surfers.
- *Uncontrolled access to profiles.* Most social networks allow for partial or full disclosure of data related to the user's profile, after which this data becomes available to everyone, regardless the data owner's consent or wish.

[24] http://www.coe.int/t/dghl/standardsetting/DataProtection/News/Web%20tacking.pdf, last time visited in November 2013.

[25] Nowadays usage of mobile computers, smart phones and other IT devices contributes to further development of the trend to analyze the users' profiles, which indirectly means abuse of the users' personal data.

- *Malware* is actually a sort of a computer program that gets installed on the user's program by itself without the user's knowledge. The program gathers important information stored on the user's computer, such as bank codes for working on the internet or details from the user's credit card. Further on, the user's internet connection is used to send this data to criminals who use this data for illegal activities.

- *Identity theft.* It has been happening quite often recently that an internet user identifies a new/dual identity in digital form, depending on whether it is the user's first time to create a profile or the user already has one profile. It all comes down to somebody else using the user's identity, not the user him/herself.
- *Contextualized advertising.* – Some services (as Google ads) based on the user preferences in visiting particular sites or reading a particular contents (although the preferences are not explicitly or consciously set by the user, but they are result of the browsing history, page viewing and ad clicking history) try to serve ads that matches the contents of the browsing history. These practices might be considered as non acceptable in context of privacy.

- *Installation and usage of "cookies" without consent of the social network user.* Basically, there are options for the website to use a number of *cookies* which enable it to monitor the activities of its users. Thanks to these tools, the social networks can track the connection point of the user, the hour of getting connected, the device the user had visited the site with (fixed or mobile devices), the operation system the user is using, the most frequented pages within one website, the number of clicks etc, and a great deal of other items of information which, basically, reveal details about the user's lifestyle, interests, needs, requirements etc.

- *Abuse* - When personal data is available on the Internet, people can misuse it or find a way to abuse it, sometimes even blackmail the owner of the data. These people do not necessarily have to be acquaintances of the user, so, caution is advisable.

    - *This might be reflected regarding the digital fingerprints (Technologies that deploy an algorithm that analyzes a large number of technical characteristics and settings to generate a unique identifier that can identify a specific* *computer because more in Europe and less in USA an IP address may be considered as "personal data"; Unique DFs could be linked to identifiable individuals; machine-IDs (Digital Fingerprint or Device ID) could be compiled with other more sensitive information to create profiles and could be cross-referenced to learn more about some person etc.;*

- *Social –networks Plug-ins as applications that on easy way allows sharing of contents, preferences etc. The privacy in term of plug ins might be endangered by the user itself (non-aware of consequences of revealing personal data through use of plug-ins), user – by – user (intentionally or unintentionally)where for example tagging of some person on a photo may allow access to the contents of it to the 3rd party otherwise not connected to the subject on a photo; and Application privacy breach in case user may use application or plug-in from a third party-developer that use different pattern of privacy security (functionality and transmit policy of the plug-in)than the one declared by the social network; and privacy breach by the social network because usually there is no possibility to compare previous privacy options and preferences to the newly introduced one including the functionality and transmit aspects of the plug –in on a network.*

- *Terms of use are difficult to understand.* Many social networks issue poorly written terms of use that are more apt to confuse than to clarify. They often run away from responsibility, and their terms can be changed without notifying the users. And who owns the data if the social network service ceases to exist?

- The use of personal data to build comprehensive profiles on individuals. Facebook and Google are only the most familiar businesses premised on systematically collecting personal in order to sell targeted advertising based on profiles. The unfolding Big Data trends comes with new opportunities for companies, and increased risks to privacy.

Macedonia

Beside their basic usage, social networks are also being used for other purposes rather than the original ones. Thus, business companies have been increasingly using these networks for enhancement of communication with their clients, for personal marketing and for turning their employees into so called "brand ambassadors"[26], which is a reality in Macedonia. However, the Directorate does not practice this type of application of the networks. Taking into account the fact that distribution of business data and information through private social networks is a reality, it is the business sector that should pay greater attention to this application of the networks and to protection of the personal data that is available on the networks, and accordingly, subject to being misused and abused. This application of the networks is actually a new field where the Directorate could act as protector of peoples' personal data.

The State Office for Statistics, in compliance with Eurostat's methodology for statistical research, conducts surveys related to social networks and their usage by citizens, businesses and public sector, and provides quantitative analyses, some of which are presented above.

In the Republic of Macedonia there are nearly 1.000.000 registered profiles only on Facebook[27], i.e. this social network is being used by 48% of the population (out of which 92% use it actively). According to the data of a survey conducted by the Rating Agency, conducting an internet poll on a sample of 800 respondents (users of Facebook), an average user of this social network spends more than 3 hours per day logged on this network[28]. Hence, the risk factor of data abuse is quite high. According to the data from this survey, this network users do not yet actively attach themselves to brands, but the businesses' activities related to marketing on the social networks are far from negligible. In addition, having in mind that in future businesses are most likely to intensify their marketing activities

[26] https://www.taylorwessing.com/globaldatahub/article_social_media_enterprise.html, last time visited in November 2013.

[27] http://www.slobodnaevropa.org/content/na-balkanu-facebook-koriste-najvise-u-srbiji-/24909738.html , last time visited in December 2013.

[28] http://it.com.mk/koj-e-prosechniot-makedonski-korisnik-na-facebook/, last time visited in October 2013.

on the social networks, it is only the matter of time when the issues related to personal data protection will become “heated topic” and will have to be addressed.

3. Cloud computing

This has been number one issue in ICT: *cloud computing*. Nowadays almost everybody uses the internet, and therefore he/she is most likely included in this or that way in the “cloud”. Updating your profile on the Facebook, using an application for an online office, uploading databases on online storing services - these are all ways of using the “cloud”. Cloud computing is of crucial significance for modern businesses, for by using the services offered by the “cloud”, they can drastically reduce their operation costs. This concept makes it possible for even start-up companies to enter big markets without risking incurring start-up costs. Cloud computing is bound to bear more significance in future. The International Data Corporation (IDC[29]) predicts that 80% of the new commercial corporation applications will be distributed into “cloud” platforms, which means that cloud computing services are of huge importance for the internet we have nowadays.

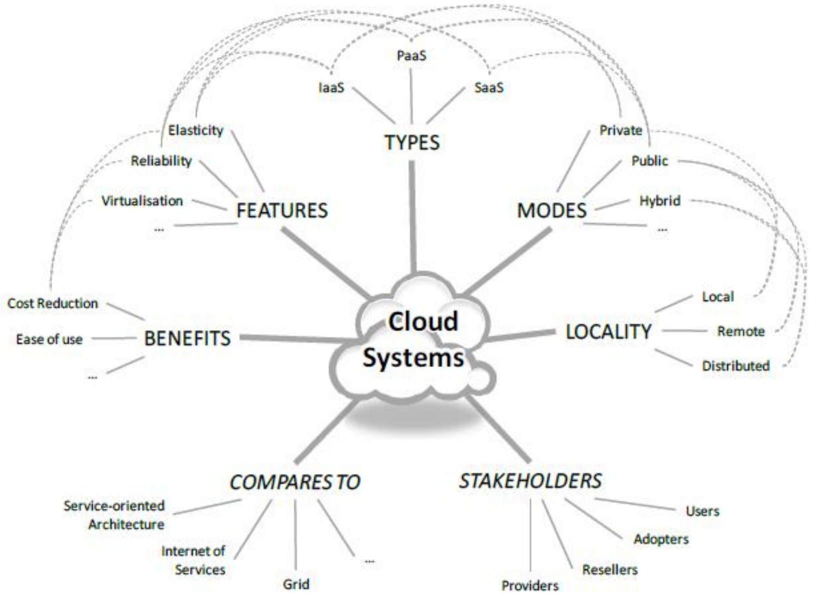


FIGURE 1: NON-EXHAUSTIVE VIEW ON THE MAIN ASPECTS FORMING A CLOUD SYSTEM

Title of the figure: Non-exhaustive view of the main aspects forming a cloud system

[29] http://www.idc.com/ , last time visited in October 2013.

Source for figure 1: http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf , how experts see "Cloud computing" in the report entitled: The Future of Cloud Computing - Opportunities for European Cloud Computing Beyond 2010

Global leader in provision of services are American providers. Thus, having this in mind, Europe is developing a new "Cloud computing" strategy that will facilitate the operation of businesses and will improve personal data protection[30]. The idea is that a Pan-European Cloud Computing Service could be the right and real response to the domination coming from across the Atlantic.

"Cloud computing" is a model that allows for a ubiquitous and convenient network access of "a request" to available computer resources that can be adequately and appropriately configured (for example, networks, servers, storage, applications and services) which can be quickly made available and free to use, with minimum efforts for their handling or interaction with the service provider. This Cloud Model consists of 5 basic characteristics, 3 servicing models and 4 distribution models[31].

	Managed by	**Owner of the infrastructure**	**Hardware available**
Public	CSP (Cloud Services Provider)	CSP (Cloud Services Provider)	NO
Private, external	CSP (Cloud Services Provider)	CSP (Cloud Services Provider)	YES
Private, internal	Internal Organization	Internal organization	YES
Hybrid	Mixed	Mixed	CSP (Cloud Services Provider)

Table 2 - Classification of types of "Cloud"[32]

[30] https://ec.europa.eu/digital-agenda/en/pillar-vii-ict-enabled-benefits-eu-society/action-109-develop-and-implement-public-service , last time visited in December 2013.

[31] http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf, definition of the National Institute of Standards and Technology (NIST) which is preparing standards that will be used by Federal American Agencies, September 2011.

[32] Internationally adopted typology, NIST standards inclusive.

Major characteristics, but the list is non-exhaustive

1. *On-demand self-service.* - The user is able independently, without an interaction by a person from the service provider, to use various IT capacities.
2. *Broad network access.* - The capacities are available through the network and by using various clients' platforms (computers, mobile phones, tablets, etc.).
3. Resource pooling. – The resources (both physical and virtual ones) of the provider of computer services are simultaneously available for a number of users with different needs and they are distributed according to the users' needs. As a rule, the user does not know the exact location of the resources he/she is using, nor can he control them, but it is possible to establish their likely location (for instance; a state, a region, a data centre etc).
4. *Extreme elasticity of the services* – The scope of services being used in a cloud can rapidly increase and/or decrease, depending on the level of demand. The user generally has a feeling that the choices are infinite and that they can meet his/her needs at any time.
5. *Measurable services* - The systems providing the services in the cloud also automatically provide information regarding the extent of usage of the respective services. This extent can be measured and controlled, and both the service provider and the service user can be informed thereof.

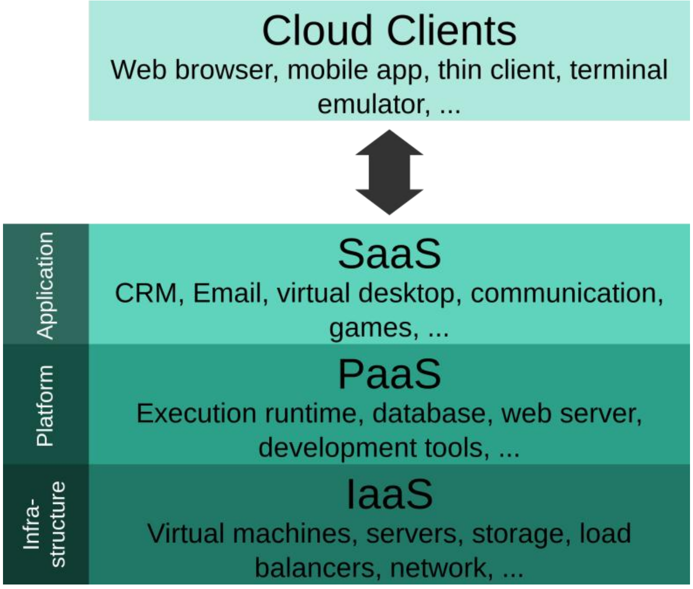
Models of services:

Three major service models in a "cloud" have been identified (although others are also present) that have been, more or less, pretty similarly defined, but basically they mean the following:

- Software as a Service (SaaS). – This is a model where a software hosted by the service provider is being distributed and made available for the service user as an application distributed through networks, most commonly through the internet. The user can not influence or control the infrastructure he is using, which applies to the network, the servers, operational systems, storage or the applications' features, except under special circumstances.
- Platform as a Service (PaaS) – The user can create his own applications by means of tools and resources such as program languages, libraries, services

and various tools, but can not control or manage the operational systems, storage. In other words, the user can control the applications' features, but not the IT infrastructure that is being used in the cloud.

- Infrastructure as a Service (IaaS)[33] - The user applies hardware resources (for data processing, storage, networking etc.) onto which he can by himself install and use computer programs and applications. It is commonly a standardized offer which the service provider offers to the users "on demand". The users can post their own Web-based interface which acts as an IT handling console. In this service, too, the user can not control the IT infrastructure.


Cloud Clients
Web browser, mobile app, thin client, terminal emulator, ...
Application
SaaS
CRM, Email, virtual desktop, communication, games, ...
Platform
PaaS
Execution runtime, database, web server, development tools, ...
Infra-structure
IaaS
Virtual machines, servers, storage, load balancers, network, ...

Author of the graph: Bikeborg

The data from literature emphasize that all of these three models of services have one thing in common, and that is virtualization. Thus, IaaS is described as virtualization of servers, storage and networks, PaaS (in a way), is virtualization of a combination of services of IaaS and SaaS. And last, SaaS is described as virtualization of the level of applications by using meta-data.

[33] Nicholas Carr, the author of the article "Does It Matter", in 2006 for the first time used the expression "Hardware as a Service" in order to describe the services such as the Amazon's "cloud" at Amazon.com -Elastic Compute Cloud (EC2). This expression is a forerunner of the expression IaaS.

Models of implementation:

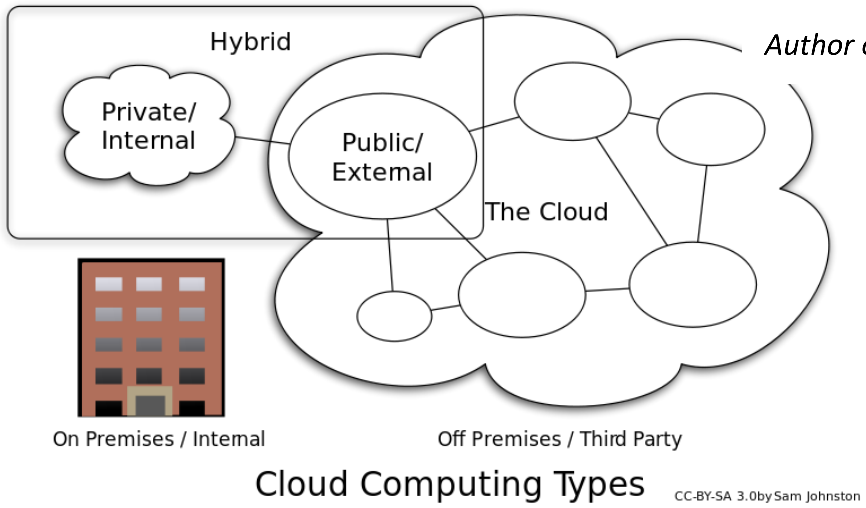
The services in the cloud can be implemented in a few ways which will be considered in the text to follow.

Private cloud – The cloud's infrastructure is dedicated to one user only (who can own it, use somebody else's infrastructure or make a combination of his own infrastructure and somebody else's one, to possess it in his rooms or outside them), or he is securely isolated from all the other users.

Common cloud – it refers to a cloud infrastructure that is divided among organizations, members of a particular community, employees and the like, entities that generally share a common need for security, privacy, functionality and suitability. This structure can be managed by one or more organizations, or a third party or a combination of the previous ones. The infrastructure, as in the previous case, can be set in the user's rooms or outside them.

Public cloud – It is defined as a set of flexible and elastic capacities offered to the external users by application of internet technologies. This is an open-type cloud and is designed for the wide public. Usage of public cloud generates wide-scope economy and shared usage of the same resources, which, in the long run of the things, leads to reduction in expenditures and increment in the choice of technologies that will be used for the services needed. In a public cloud all the users have equal rights regarding usage of resources (the resources can be used both by public and private institutions, many different institutions can use them at the same time etc.). Therefore, it is impossible to guess and guarantee exactly where the data for which the service is used will be located and stored. This structure can be managed by a business entity, an academic entity, a government institution or a combination of the three.

Hybrid cloud - it is a selection of some of the above mentioned models of implementation which continue to be independent, but due to certain reasons they are obliged to intercommunicate. Reasons for this could be application of a particular standard, application of technologies etc.



Author of the graph: Sam Johnston

Macedonia

What is important to point out is that in practice there are certain conditions or occurrences that have not yet been perceived as "Cloud computing", but for which, *de facto,* the issue of personal data abuse is extremely important.

A rising trend among the online services in the business sector is e-shops[34], although a practice for doing business on internet is around for some time already. From viewpoint of personal data protection, the following data is important. In accordance to data of the International Cards System during the year 2011 some 77.000 transactions in electronic trade were conducted, whereas in the year 2013 this figure is expected to reach the number of 265.000 transactions[35]. Since 2007, 300 companies in Macedonia selling goods online have been registered. It is extremely important to achieve successful online transactions at real time, in cases when sometimes a few users need the services of one provider, when there is a need of rapid data check-up in order to realize the transaction; these are all cases when engagement of massive IT potentials is a must. For all these situations the solution lies in "Cloud computing"[36]. These are all reasons worth enough to draw our attention to this trend.

[34] http://www.kanal5.com.mk/vesti_detail.asp?ID=27621 , lat time visited on January 9th 2014.

[35] The new analyses are not available at the time of writing this report.

[36] For example, Amazon applies "Cloud Computing" to accomplish its activities.

Also, on a global level, we are all familiar with the cases of establishment of systems for reporting violations and cases of corruption (*Whistleblowing*) within a company. Quite often these systems are created online, thus being treated as systems in a cloud. Since the entities reporting the cases are natural persons, the need of personal data protection comes by default. As part of this Analysis, we have not conducted detailed surveys on this issue, but in the country there are some generally well known services for reporting corruption[37]. In Sweden, for example, the authorities for personal data protection are in charge of this type of systems. Namely, when an organization which is not a state authority, but by law is entitled to receiving reports on corruption, wishes to introduce this system, it is issued by the above mentioned authorities for personal data protection a license to apply the system[38]. It is of crucial importance to provide protection of privacy and movement of data in an environment that is not by default treated as free from risks of personal data abuse.

IV. LEGAL FRAMEWORK

1. National legal framework

For the purposes of this Analysis, the below mentioned regulations were consulted to a greater or smaller extent.

The right on protection of personal data is regulated with Article 18 from the Constitution, which lays the foundations for guaranteeing security and confidentiality of personal data and protection against violation of the citizens' personal integrity.

If looking at it in details, the sphere of personal data protection is governed by the following regulations:

Laws

1. Law on Personal Data Protection ("Official Gazette of the Republic of Macedonia" No. 7/05, 103/08, 124/10, and 135/11)

[37] For instance, on the web site ttp://www.transparency-watch.org/reports/submit one can file a corruption report, but there is no evidence whether and in which way the rules are regulated and the measures for personal data protection are carried out.

[38] http://www.datainspektionen.se/Documents/vagledning-whistleblowing-eng.pdf, last time visited in December 2013.

2. Law on Ratification of the Additional Protocol to the Convention for Protection of Individuals Against Automatic Personal Data Processing, With Respect to the Supervisory Bodies and the Cross-border Transfer ("Official Gazette of the Republic of Macedonia", No. 103/08)

3. Law on Ratification of the Convention for Protection of Individuals Against Automatic Data Processing ("Official Gazette of the Republic of Macedonia", No. 7/05)

4. Sector laws from a number of areas (electronic communications, education, health, notary services, securing properties and persons, tourism, trade, banking etc.)

Rulebooks and guidelines

1. Rulebook on technical and organizational measures for provision of confidentiality and protection when processing personal data - refined text ("Official Gazette of the Republic of Macedonia" No. 38/09, 158/10)

2. Rulebook on the form and contents of the form for notifying somebody of personal data processing and on the way of entering the information into the Central Register of sets of personal data - refined text ("Official Register of the Republic of Macedonia" No. 155/08)

3. Rulebook on the contents and form of the Act on the way of performing video surveillance ("Official Gazette of the Republic of Macedonia", No. 158/10)

4. Rulebook on the form and contents of the form for keeping records of conducted transfer of personal data ("Official Gazette of the Republic of Macedonia", No. 158/10)

5. Rulebook on the manner of performing inspection supervision ("Official gazette of the Republic of Macedonia", No. 158/10)

6. Rulebook on the form and contents of the invitation for education, the way of implementing education, and the way of keeping records of it ("Official Gazette of the Republic of Macedonia", No. 158/10)

7. Rulebook on the way of keeping single records of misdemeanors, sanctions pronounced and decisions made in misdemeanor procedures, as well as the way of gaining access to the information contained in the records ("Official Gazette of the Republic of Macedonia, No. 136/08)

8. Rulebook on the form, the form and contents of the identification card and the way of issuing and withdrawing it - refined text. ("Official Gazette of the Republic of Macedonia, No. 143/08) [Undertake it]

9. Rulebook on the form and the contents of the request to establish infringement of the right to personal data protection ("Official Gazette of the Republic of Macedonia, No. 144/11)
10. Instructions on the manner of implementation of external control - Act of the Directorate
11. Instructions amending the instructions on the manner of implementation of external control - Act of the Directorate
12. Report on conducted (internal or external) control of the information system and the information infrastructure - a form, Act of the Directorate

Regarding social networks and "cloud computing", general regulations on personal data protection are applied, whereas in each case separately it is necessary to check the applicability of the sector law, too.

The Analysis resulted into general recommendations for some amendments in the legal framework, which is listed in the part "Conclusions and Recommendations".

2. International legal framework

Additionally, beside the Law on Personal Data Protection, the legal framework for personal data protection in the Republic of Macedonia includes the European Convention on Human Rights and the Convention of the Council of Europe No. 108/1981 on Protection of Individuals, which refers to automatic personal data protection, as well as the additional Protocol to this Convention on Supervisory Organs and Cross-Border Transfer of Data, ratified by the Parliament of the state.

National legislation has also been harmonized with the European legislation (Directive 95/46/EC of the European Parliament and the Council on protecting individuals with respect to personal data protection and free flow of such data), under the EU accession procedure of our country[39]. In that respect, the Directorate applies, legislatively and in practice, all the novelties associated with personal data protection, and takes active participation in the process of defining new trends for more efficient protection.

[39] http://ec.europa.eu/justice/data-protection/law/index_en.htm, last time visited in December 2013.

The novelties introduced in Europe are fully being monitored, for the rules that will be proposed shall be implemented in the national legislation, too. Accordingly, consideration is taken of the proposal to raise the level of regulation from Directive into Regulation, reaching thus horizontal compliance of the rules on personal data protection with the new, modern technologies applied by the companies in EU, as well as by those offering services to the citizens throughout Europe, especially in the online contacts.

Proposals to raise the accountability of the controllers and data processors in general, as well as introduction of new requirements proposed with the new Regulation, including preparation of documentation for data processing, development of assessment criteria for privacy influence, (privacy-by-design/default), shared responsibility of the data processors - these are all novelties that have to be incorporated into the national legislation. This applies to the other aspects of the Regulation that might involve contextual changes. Providing, of course, the Regulation is adopted such as proposed[40].

The proposal for a new directive on Cyber Security[41] shall be considered, too. Proposals to introduce obligations for the companies to introduce technical and organizational measures, obligation to conduct security revision and obligation to report infringements to the regulator, these are novelties that will additionally necessitate context changes, in particular because of the proposal to apply this directive in companies and cases such as: commercial (trading) companies, paying on the internet, social networks, internet browsers, Cloud computing services, shops selling software applications, electrical power suppliers, transport/logistics-related companies, loan-granting institutions and stock markets, health-related organizations.

With the purpose of keeping up with the trends in Europe, it is important to monitor the strategic positions of the European Commission (EU Strategy on Personal Data Protection) in this sphere, with respect to: 1) standards simplification and certification of cloud computing,

[40] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52012PC0011:en:NOT, last time visited in December 2013.

[41] http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security, last time visited in December 2013.

2) development of new models, agreements and clauses, and 3) initiating European Cloud Partnership.

V. METHODOLOGY

For preparation of the report, traditional research methods were applied involving analysis of primary and secondary legal and other sources (for instance: national and EU legislation, official strategic documents and practice). With a view to obtaining a better idea of the trends that are subject of interest of this analysis, additional information sources were used (websites, blogs and other state-of-the-art formats) in volume that allows for making relevant conclusions.

With the purpose of assessing the conditions in the Directorate and the personnel's readiness to deal with the issue of privacy protection on social networks and in Cloud computing, a survey was conducted by means of a questionnaire filled in by the Directorate staff[42], as well as interviews with the relevant employees.

Views and definitions of institutions such as NIST and the expert group of the European Commission regarding privacy, social networks and Cloud computing, have also been taken into account and appropriately addressed in the Analysis. When relevant, academy resources were also taken into consideration.

To a limited extent, technical sources have also been referred to (websites and services of technical companies such as Oracle, Hewlett Packard, Microsoft, Facebook etc.) that are commonly used at the moment.

Concerning legal framework, the regulations from Chapter IV, point 1 and point 2 have been consulted, too, so that apart from the Law on Personal Data Protection and Sector Laws, as well as the by-laws, the Directive on Personal Data Protection was also referred to, together with the Analysis of conformity of the Law with the Directive, the proposal for Regulation on Personal Data Protection and other documentation. The position of the Working group from Article 29, the Supervisor's documentation regarding personal data protection, and the Berlin Group's views, were also taken into consideration. The relevant practices of the

[42] The questionnaire was base for gathering empirical data for the preparation of this Report.

European Court of Justice (ECJ) were consulted, although not directly included into the Analysis. These practices, in the context of the issues addressed by this Project, could be used as associated documentation (manuals, guidelines and the like) that shall be prepared for the needs of the Directorate.

There should be no doubt that all the information and data used in this Report had been analyzed only from the standpoint of personal data protection on social networks and "Cloud Computing".

VI. ANALYSIS OF CURRENT STATE

The directorate handles cases related to social networks and *"Cloud Computing".*

Through the Complaints and Appeals Department, the citizens can submit requests for their privacy protection. Provided the request is relevant and the Directorate is held competent, the official shall contact the respective social network. Most success has been evident with the social network Facebook with which an informal cooperation is going on. Despite the fact that the cooperation is running fairly well, lack of formal documents (headed letter, for instance) could be considered as a drawback. This in particular applies to other networks the Directorate had attempted to cooperate with, but practice had shown disinterest of the provider for that sort of cooperation.

The above findings are compared to the state of affairs in Norway. It is obvious that there is no difference in regard possibilities of the data protection authorities to communicate and cooperate with social networks when abuse or likelihood to appear one.

1. Complaints submitted to the Directorate

In the year 2013, for the period between January 1st 2013 and December 31st 2013, a total of 404 complaints, both from physical and legal entities, based on all grounds, had been submitted to the Directorate. Some of these complaints refer to abuses made by social networks. The Directorate handles these complaints, too. During 2013, a total number of 252 complaints on abuse of personal data by social networks had been handled. The Directorate generally handles cases that cover most common types of abuse on social networks, such as complaints for deletion of fake profiles on Facebook (187/252) or deletion of hacked profiles (43/252). The Directorate had also handled complaints for disclosure of IP address, unauthorized publication of photographs, abuse of minors' personal data etc. Out of 252 complaints submitted to the Directorate for the above mentioned period, a total of 218 had dealt with abuse on social networks. With the intensified activities of the Directorate aimed at raising people's awareness of possible personal data abuse on social network, this trend is very likely to continue growing in future, bearing especially in mind the Directorate's strategic approach to strengthen the activities in this area.

With reference to this statement, below is listed some statistical data concerning the number of complaints, i.e. cases being handled by the Directorate in the course of the years past. So, in the year 2012, for the period between January 1st 2012 and December 31st 2012, a total of 385 complaints had been submitted to the Directorate, out of which 207 were complaints for personal data abuse on social networks[43]. Regarding personal data abuse on social networks, 118 complaints were submitted for deletion of fake profile on Facebook, 49 complaints for cracking a user's name or profile password on Facebook, 9 complaints for removal of videos and photographs from You Tube, and 31 complaints of various kinds (deletion of an e-mail address, cases forwarded by the Ministry of Interior to be settled, and other types of abuse on social networks and issues)[44].

For the period between January 1st 2011 and December 31st 20`11, 363 complaints had been submitted to the Directorate. The complaints were about personal data abuse, and out of the total of 363, 127 were about personal data abuse on social networks[45]. Regarding personal data abuse on social networks, 87 complaints were related to deletion of fake profile on Facebook, 12 about cracked profile, 3 complaints were submitted by a group on Facebook for abuse of personal data, 3 complaints related to You Tube and 11 other complaints were related to deletion of e-mail addresses, resent cases to be handled by the Ministry of the Interior, and other types of abuse on social networks and issues[46].

[43] Report on operation of the Directorate for Personal Data Protection for the year 2012.

[44] Report on operation of the Directorate for Personal Data Protection for the year 2012.

[45] Report on operation of the Directorate for Personal Data Protection for the year 2011.

[46] Report on operation of the Directorate for Personal Data Protection for the year 2011.

As a rule, it is natural persons who submit complaints rather than legal entities, the ratio being 10:1 respectively.

Counseling

In its communication with the individuals who had filed a complaint for personal data abuse on social network, in addition to conducting a procedure to support the individual concerned, the Directorate also plays a counseling role. Thus, by implementation of the communication strategy and various types of cooperation with other institutions and the non-government sector, the Directorate additionally informs the general public about issues associated with social networks. However, fact is that the counseling role of the Directorate necessitates additional improvements, and in that context establishment of a web platform via which this role of the Directorate will be accomplished is highly recommended.

2. Inspection supervision

In compliance with the Law on Personal Data Protection, the Law on General Legal Proceedings, the Rulebook on Technical and Organizational Measures for Provision of Confidentiality in Personal Data Processing, the Rulebook on Inspection Supervision, the Sector legislative referring to the respective personal data controller who is being supervised, as well as the Opinion 05/2012 on *Cloud Computing* dated July 2012 and the Working Document on *Cloud Computing* - Privacy and issues related to data protection "Sopot Memorandum" dated April 2012[47], the Directorate, via the Sector for Inspection Supervision (see Chapter II of this Analysis), conducts inspection of the personal data controllers. This inspection supervision is carried out by authorized inspectors employed with the Directorate. They perform three types of supervision: regular supervision, special supervision and control supervision.

Regular supervision is performed based on an annual program for inspection supervision and is realized following monthly operation plans for inspection supervision, which contain

[47] Working Paper on Cloud Computing - Privacy and data protection issues - "Sopot Memorandum" - 51st meeting, 23-24 April 2012, Sopot (Poland).

details regarding the controllers to be supervised, the sets to be supervised and date of commencement of supervision.

The procedure for supervision on a regular basis commences by sending a Notification of inspection supervision to the respective personal data controller. In the Notification, the controller is informed about the day of inspection supervision and his/her obligation to submit, one day before the supervision date, a filled in Main Checklist[48] published on the Directorate's web site. This list contains 28 questions grouped under two points: 1) Questions for the controllers, and 2) Questions about the sets of data. The information contained in this list is basis for conducting on-the-spot supervision, for which the inspector prepares himself thoroughly. Prior to realizing the on-the-spot visit, the inspector shall check whether the formal requirements laid down in the regulation on basis of which the supervision is conducted are met, which are basically related to the supervision procedure, the legal requirements related to the personal data controllers and the sets of data, and the like (e.g. if the controller had been duly notified of the supervision, if he had timely submitted the Main Checklist, if he is registered in the *Central Register of Controllers and Sets of Personal Data*[49] and the like). The Inspector shall also prepare himself for the contents of the supervision, which he does by studying the legislation of the sector in which the controller works, as well as the controller's profile. The profile is created by searching information about the controller through "Network (WWW)" and by communication with the Central Registry of the RM, with reference to the Register of Trade Companies and Other Legal Entities. In some cases problems in communication with the Central Registry have been reported, due to which some data is either delayed or unavailable. I believe that the Central Registry is obligated[50] to provide the Directorate with relevant data for free, having in mind that the Directorate is an institution funded by the budget of the state and

[48] http://dzlp.mk/mk/inspekcija.

[49] This Central Register is a database kept by the Directorate. It differs from the eponymous institution entitled Central Registry of the RM, which is kept for trading companies and other legal entities, from the The Register of Pledges, the Register of Annual Accounts, Leasing Register and other types of registers.

[50] In compliance with Article 18a from the Law on Central Register («Official Gazette of the RM, No. 50/201, 49/2003, 109/205, 88/2008 and 35/2011).

from other sources[51]. In case the delays in communication are based on differences in interpretation of the regulation laid down in Article 18a from the Law on Central Registry, with respect to the question whether the Directorate shall or shall not be considered a privileged institution, it is necessary without any delay to initiate amending the quoted regulation. In this way the Directorate (its inspectors) will have a real-time (and online) access to the data entered in the Register, which will mean high level of relevancy of the data about the controller under supervision, as well as uttermost efficiency in execution of the supervision activities.

Having defined the details of the supervision visit with the officials in charge, the controller is visited on the very spot. During the visit, the inspector interviews the relevant employees/officials in charge/officer for personal data protection, whereupon the relevance of the interviewee depends on the type of set of personal data the controller is building. The supervision can be conducted in one day only, or can take place during a few days, which depends on the volume of the sets, i.e. the data the controller is collecting. During the supervision, the inspector goes through the controller's documentation, inspects the manner and procedures related to processing personal data, but also gathers evidence to support findings indicating irregularities in the work of the respective controller. Evidence can be documents such as photocopies of the Acts governing storage and processing personal data, agreements, statements, authorizations, photo documentation created on the spot, and other items that can be used as evidence. The supervision findings shall be recorded in Minutes on the supervision conducted, which shall be completed in writing within 30 days on completion of the supervision (read: last delivery of the last piece of evidence provided by the controller for the purposes of the supervision). It seems that regarding terms for evidence delivery by the controllers, there is quite big flexibility. Concerning *Cloud Computing*, it is recommended to insist on diligence and on short-notice evidence delivery terms[52]. The supervision procedure shall end with preparation of Minutes on the supervision conducted and with decision made by the inspector. According to that decision, the inspector can close the case, make decision regarding the supervision with

[51] Article 48 from the Law on Personal Data Protection («Official Gazette of the Republic of Macedonia", No. 7/05, 103/08, 124/10, 135/11).

[52] To consider the possibility for revision of the Regulation in this direction.

which he will entrust the controller with the task of eliminating the irregularities[53], and in case of violation of the Law on Personal Data Protection, he can take further measures against the controller by initiating a misdemeanor procedure before the Misdemeanor Commission, or by initiating relevant procedure before another competent organ (for instance, to press charges against the controller before the Public Prosecutor, based on knowledge/suspicions about committed criminal act).

So far, there has been no case that during inspection supervision the controller had refused to provide the documents requested from him. Yet, in case the inspector encounters such a situation, he is authorized to note that the controller does not have the needed information/documentation, and additionally, the inspector is entitled to initiating misdemeanor procedure on account of the controller's disabling the inspector to do his work.

Supervision can be conducted by one inspector, but the inspection can be carried out by a team of inspectors. In that case, one of the inspectors who had been entrusted with the case is the one in charge and he runs the whole case, from the beginning to the end. The inspector in charge signs the documentation related to the relevant case. When needed, the team is strengthened with an inspector from the field of IT. This practice can be considered as a positive one.

Regarding *Cloud Computing*, during the year 2013 two supervisions were conducted, including services in "the cloud". In one of the cases, the controller was user of "cloud" services, while in the other case there was a service provider in "cloud". In both cases there was transfer a cross-border transfer of data.

The Directorate is staffed with employees well trained to perform supervision of *Cloud computing.* The area that needs improvements is the way in which one can gain information whether a particular controller applies *Cloud computing*. Also, having in mind the complex nature of the issue, a continuous monitoring of the developments in this area and permanent education of the inspectors is a must, although in the course of July 2011 the

[53] The controller has a court protection, with the possibility to take legal actions before the Administrative Court regarding the inspector's Decision.

inspectors were certified with ISO 27001. By acquiring this Certificate, the inspectors gained higher capacity for supervisions in the complex IT infrastructure of the controllers and data processors in diverse spheres.

Special supervision is conducted when initiated by a state administrative body, legal or physical entity, i.e. a filed complaint, and in case the inspector suspects infringement of the Law regulations. Unlike regular inspection supervisions, visits that have the character of special supervisions are not part of the working plans of the Directorate. They are basically ad hoc visits which do not necessarily have to be previously announced. They can refer to control of the operation of the personal data protection controller to be supervised, but the logics behind this type of supervision is control of the particular case reported and identified by the Directorate, which is too urgent to be included into the planned documentation.

Control supervision is supervision whose purpose is to check the conduct of the controller after finding irregularities with his work, it means, to see whether the controller had carried out the tasks assigned to him by the inspector, aimed at elimination of the irregularities, i.e. if he had taken appropriate measures to reduce the risks and threats of future abuse of the personal data whose controller he is. At the very moment of finding the irregularities, the controller is given a time period within which he is expected to eliminate the irregularities and remedy the situation. The supervisor can give an advance notice of the visit, but as a rule it is not necessary. The next supervision period is 15 days and it starts running from the last day of the time period given to the controller to remedy the situation. For this control supervision other Minutes are composed, stating the extent to which the controller had performed the task. Providing the controller had not, partially or fully, completed the assignment, the inspector is entitled to initiating misdemeanor procedure.

In the course of the past three years, there is an increase in the number of cases handled by the inspectors, which is result of the intensified activities of the Directorate. The table below illustrates the trend in figures.

	Inspection supervision 2011-2013 as per the Annual Reports on the Directorate's Operation					
Year	Regular supervision	Special supervision	Control supervision	Cases transferred from the previous year	*Cloud computing*	Total without transferred cases
2011	107	32	7	18	-	146
2012	273	95	-	28	-	368
2013					2	

Counseling and education

The Directorate also has a counseling role in the field of *Cloud computing*, both towards the subjects inspected and the wider public.

Additionally, in the course of the supervision, the inspectors as well as the individuals who had made the irregularities, the latter after being included in the Minutes but before being pronounced a sentence, are entitled to attending education about personal data protection, and in particular with respect to the infringements they had made.

With the amendments in the Rulebook on inspection supervision introduced in 2011, the inspectors are legally obliged to provide the controllers who had had irregularities in their work, with education during the very supervision, which is a big step towards timely response. This approach to issues in digital surroundings is of particular significance - quick and efficient reaction.

VII. RECOMMENDATIONS AND CONCLUSIONS

1) To continue with promotion of the role and position of the Directorate in the field of personal data protection in general, so that the public would be better acquainted with the competencies of this institution, which would raise the public awareness of this issue.

2) To carry out activities for assessment of the public awareness of the right of personal data protection on the internet, and to work on raising this awareness.

3) With a view to planning and monitoring the situation, to establish cooperation with the State Statistical Office, and in that context to introduce into the questionnaires analyzing the information society questions that would allow monitoring the

situation regarding *Cloud computing* and social networks, for business entities, public administration and physical entities.

4) To improve the Directorate's cooperation with other institutions which are held competent in the sphere of electronic communications, such as the Agency for Electronic Communications, the Ministry of Informative Society and Administration, the Ministry of Transport and Communications, the Central Registry etc.

5) To improve the cooperation with organizations from the business sector, such as social networks or providers of *Cloud computing*, by signing Cooperation Declarations or Memoranda.

6) To improve the cooperation with educational institutions on all levels (the Ministry, local authorities, schools) with the purpose of enhancing the teachers', professors', the youth's and the children's awareness of the right of personal data protection on social networks. Additionally, this recommendation to be included into the already existent Project dealing with privacy in education and financed by the EU.

7) Since at present, from organizational aspect, the Directorate meets all the needs, in order to increase the efficiency of the operation with the present staff, the Directorate recommends improvement of the tools available in the Directorate. To update the Checklist that is sent to the controllers prior to conducting supervision on a regular basis, by introducing questions related to usage of *Cloud computing* and social networks, for the needs of the controllers of personal data. In that way the controllers will get information about usage of these services even before the inspection supervision starts. This is particularly important in the context of *Cloud computing*, because usage of these services is information that is seldom available in public sources.

8) Regarding the organizational capacities of the Directorate for handling cases related to social networks, there is a need of increase in the number of employees dealing with this issue, which can be achieved by seconding rather than by hiring new staff. This is particularly important in the context of the coming activities to be performed within this Project, such as the "Support Team" and the Web platform for assistance

for individuals whose right on privacy had been breached, i.e. their personal data had been abused on social networks.

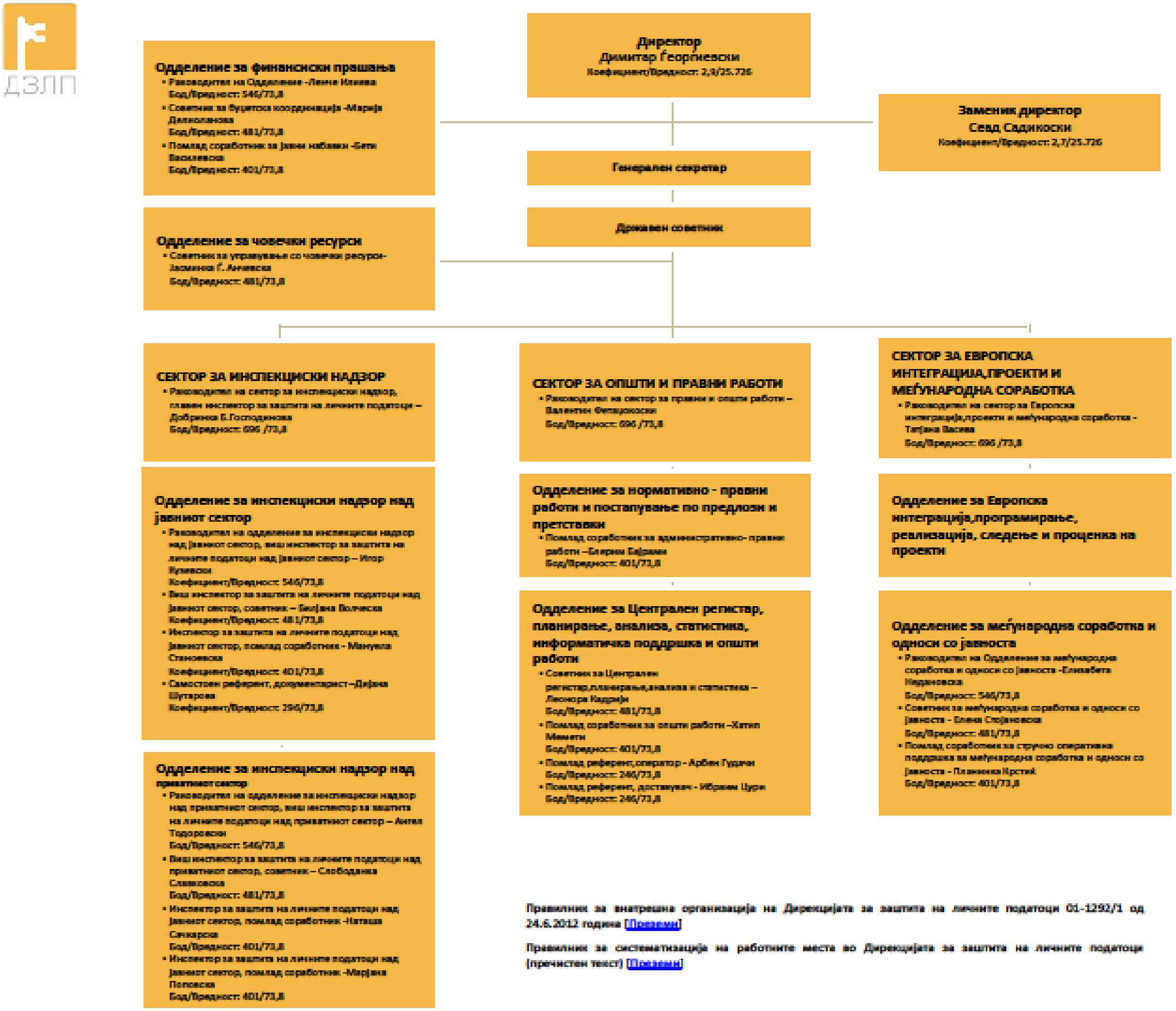
9) Even though the control over *Cloud computing* conducted with controllers that use this service is quite satisfactory, there is still need to pay better attention to the legal aspects of the protection (appraisal of the contents of the regulations that are being used/are missing in the international cooperation of the controller's partners and the controller himself).

10) To revise legislation, i.e. to treat *Cloud computing* as an across-border data transfer, and to entrust the controllers with the task of requiring an approval for transfer in order to use the *Cloud computing* services. Additionally, to introduce an obligation for the controllers to have to submit a Notification to the Directorate prior to commencement of using such services.

11) To introduce an obligation for the controller who intends to start using *Cloud computing* services to submit to the Directorate, apart from the Notification, a Checklist for the service provider and evidence of conformity of the service with the regulation on personal data protection.

12) To conduct a large-scale survey in public in order to find out people's attitudes regarding their privacy protection, with a view to appropriately directing the future activities of the Directorate.

Annex 1 – Organizational chart of the DPDP



ДЗЛП

Директор
Димитар Ѓеорѓиевски
Коефициент/Вредност: 2,9/25.726

Заменик директор
Сеад Садикоски
Коефициент/Вредност: 2,7/25.726

Генерален секретар

Државен советник

Одделение за финансиски прашања
- Раководител на Одделение -Ленче Илиева
Бод/Вредност: 546/73,8
- Советник за буџетска координација -Марија Делиоланова
Бод/Вредност: 481/73,8
- Помлад соработник за јавни набавки -Бети Василевска
Бод/Вредност: 401/73,8

Одделение за човечки ресурси
- Советник за управување со човечки ресурси-Јасминка Г. Анчевска
Бод/Вредност: 481/73,8

СЕКТОР ЗА ИНСПЕКЦИСКИ НАДЗОР
- Раководител на сектор за инспекциски надзор, главен инспектор за заштита на личните податоци – Добринка Б.Господинова
Бод/Вредност: 696 /73,8

Одделение за инспекциски надзор над јавниот сектор
- Раководител на одделение за инспекциски надзор над јавниот сектор, виш инспектор за заштита на личните податоци над јавниот сектор – Игор Кузевски
Коефициент/Вредност: 546/73,8
- Виш инспектор за заштита на личните податоци над јавниот сектор, советник – Билјана Волческа
Коефициент/Вредност: 481/73,8
- Инспектор за заштита на личните податоци над јавниот сектор, помлад соработник - Мануела Становеска
Коефициент/Вредност: 401/73,8
- Самостоен референт, документарист –Дијана Шутарова
Коефициент/Вредност: 296/73,8

Одделение за инспекциски надзор над приватниот сектор
- Раководител на одделение за инспекциски надзор над приватниот сектор, виш инспектор за заштита на личните податоци над приватниот сектор – Ангел Тодоровски
Бод/Вредност: 546/73,8
- Виш инспектор за заштита на личните податоци над приватниот сектор, советник – Слободанка Славковска
Бод/Вредност: 481/73,8
- Инспектор за заштита на личните податоци над јавниот сектор, помлад соработник -Наташа Сачкарова
Бод/Вредност: 401/73,8
- Инспектор за заштита на личните податоци над јавниот сектор, помлад соработник -Марјана Поповска
Бод/Вредност: 401/73,8

СЕКТОР ЗА ОПШТИ И ПРАВНИ РАБОТИ
- Раководител на сектор за правни и општи работи – Валентин Фетаџокоски
Бод/Вредност: 696 /73,8

Одделение за нормативно - правни работи и постапување по предлози и претставки
- Помлад соработник за административно- правни работи –Блерим Бајрами
Бод/Вредност: 401/73,8

Одделение за Централен регистар, планирање, анализа, статистика, информатичка поддршка и општи работи
- Советник за Централен регистар,планирање,анализа и статистика – Леонора Кадрији
Бод/Вредност: 481/73,8
- Помлад соработник за општи работи –Хатип Мемети
Бод/Вредност: 401/73,8
- Помлад референт,оператор - Арбен Гудачи
Бод/Вредност: 246/73,8
- Помлад референт, доставувач - Ибраим Цури
Бод/Вредност: 246/73,8

СЕКТОР ЗА ЕВРОПСКА ИНТЕГРАЦИЈА,ПРОЕКТИ И МЕЃУНАРОДНА СОРАБОТКА
- Раководител на сектор за Европска интеграција,проекти и меѓународна соработка - Татјана Васева
Бод/Вредност: 696 /73,8

Одделение за Европска интеграција,програмирање, реализација, следење и проценка на проекти

Одделение за меѓународна соработка и односи со јавноста
- Раководител на Одделение за меѓународна соработка и односи со јавноста -Елизабета Недановска
Бод/Вредност: 546/73,8
- Советник за меѓународна соработка и односи со јавноста - Елена Стојановска
Бод/Вредност: 481/73,8
- Помлад соработник за стручно оперативна поддршка за меѓународна соработка и односи со јавноста - Пламенка Крстиќ
Бод/Вредност: 401/73,8

Правилник за внатрешна организација на Дирекцијата за заштита на личните податоци 01-1292/1 од 24.6.2012 година [Преземи]

Правилник за систематизација на работните места во Дирекцијата за заштита на личните податоци (пречистен текст) [Преземи]