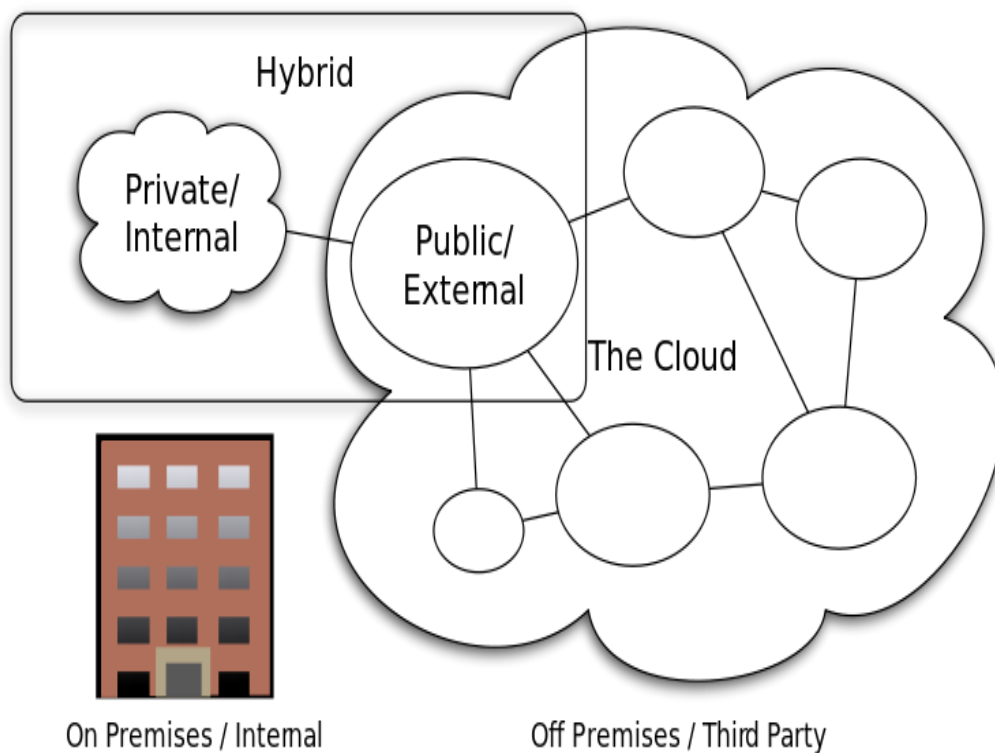


Анализа за состојбата на организациските и институционалните капацитети за заштита на личните податоци



„Техничка помош за зајакнување на
организациските и институционалните
капацитети за заштита на личните
податоци“

Скопје, февруари 2014



Cloud Computing Types

CC-BY-SA 3.0 by Sam Johnston

Оваа анализа е дел од Проектот насловен како „Техничка помош за зајакнување на организациските и институционалните капацитети за заштита на личните податоци“ кој се спроведува во рамки на континуираниот развој на Дирекцијата за заштита на лични податоци на РМ.



Проектот е финансиран од Министерството за надворешни работи на Кралството Норвешка, во рамки на билатералната соработка помеѓу Република Македонија и Кралството Норвешка.

Содржина

I.	ВОВЕД И ЦЕЛИ	3
II.	ДИРЕКЦИЈА ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ НА РМ	5
III.	КОНТЕКСТ НА ИЗВЕШТАЈОТ	8
1.	Статистички податоци	8
2.	Социјални мрежи	10
	Македонија	14
3.	Cloud computing	16
	Главни карактеристики, но листата не е исцрпена:	18
	Модел на услуги:	19
	Модел на имплементација:	20
	Македонија	21
IV.	ПРАВНА РАМКА	23
1.	Национална правна рамка	23
	Закони	23
	Правилници и упатства	23
2.	Меѓународна правна рамка	24
V.	МЕТОДОЛОГИЈА	26
VI.	АНАЛИЗА НА СОСТОЈБАТА	27
1.	Претставки до Дирекцијата	28
	Советување	30
2.	Инспекциски надзор	30
	Советување и едукација	35
VII.	ПРЕПОРАКИ И ЗАКЛУЧОЦИ	35
	Анекс 1 - Органиграм на ДЗЛП	38

1. ВОВЕД И ЦЕЛИ

Во изминатите години (повеќе од деценија) сведочиме револуција во комуникациите. Се повеќе професионалната, но и приватната комуникација се одвива on-line. Ваквите on-line се достапни и се поголем број на услуги заедно со голема количина на мултимедијални содржини. Причините за тоа се бројни, но секако главен двигател е – интернетот. Тоа е моќна и ефикасна платформа преку која давателите на услуги им нудат најразлични сервиси на потрошувачите.

Од друга страна, on-line комуникацијата е двонасочна и таа им дава можност на давателите на услуги да приберат податоци за своите потрошувачи, во обем и на начин, кои пред револуцијата, која доведе до дигитално (информатичко) општество, не биле познати. Провајдерите на услуги пронајдоа начин за зголемување на приходите, а потрошувачите или корисниците на услуги од друга страна ги прифатија погодностите на on-line услугите и се чувствува напредок или тренд на зголемена побарувачка односно понуда на on-line услуги.

Во сево ова не заостануваат ниту државите кои нудејќи on-line услуги за своите граѓани од секаков вид придонесуваат за натамошен развој на дигиталното (информатичко) општество гледајќи во овој вид на испорака на услуги средство за натамошни заштеди односно намалување на трошоците за обезбедување на услуги на граѓаните, како и средство за развој на нови и претходно недостапни услуги, често само преку интернет зашто на тој начин ќе бидат достапни независно од физичките ограничувања вклучувајќи ја територијалната ограниченост.

Затоа, не помалку важни се прашањата кои се однесуваат на ИТ инфраструктурата потребна за обезбедување на on-line услуги и сервиси за која и давателите на услуги и корисниците ќе очекуваат да биде сигурна и достапна во секое време и на секое место, ќе бидат функционални услугите, а податоците ќе се процесираат и складираат безбедно.

Така, може да се заклучи дека развојот на дигиталното општество значи и достапност односно развој на повеќе услуги и сервиси on-line кои може да се користат преку различни медиуми и тоа компјутери, мобилни телефони и слично.

Во вакво опкружување од интерес на оваа анализа се појавите на социјалните мрежи и **cloud computing** концептот во врска со заштитата на личните податоци кои неминовно циркулираат на интернет во најразлични форми и контекст. Заштитата на личните податоци е предмет на интензивна глобалната дебата, предизвикана од вонредниот развој на информатичката технологија (ИТ), постојано растечкиот капацитет на производи за чување и процесирање на податоци и нивната меѓусебна поврзаност. Дебатата е особено предизвикана од начинот на кој споменатите производи се користат.

Оваа анализа е дел од Проектот насловен како *„Техничка помош за зајакнување на организациските и институционалните капацитети за заштита на личните податоци“* кој се спроведува во рамки на континуираниот развој на Дирекцијата за заштита на лични податоци на РМ. Проектот е финансиран од Министерството за надворешни работи на Кралството Норвешка, во рамки на билатералната соработка помеѓу Република Македонија и Кралството Норвешка. Овој Проект се спроведува *со цел понатамошно јакнење на организациските и институционалните капацитети на Дирекцијата за заштита на личните податоци за подобра и поефикасна заштита на правото на приватност на социјалните мрежи, подобрување на услугите на социјалните мрежи во однос на заштитата на правото на приватност, подигање на јавната свест кај граѓаните за правото на приватноста при користење на интернетот, како и јакнење на нивното знаење во однос на современиот технолошки развој и новите прашања кои се поврзани со приватноста како што е cloud computing.*

2. ДИРЕКЦИЈА ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ НА РМ

Дирекцијата за заштита на лични податоци (во натамошниот текст: Дирекцијата) е самостојна и независна институција која е надлежна за вршење надзор над законитоста на преземените активности при обработување на личните податоци и нивната заштита, на територијата на Република Македонија.¹

Дирекцијата преку својот Директор секоја година доставува до Собранието Извештај за работата. Доколку има потреба за тоа или по барање на Собранието на РМ Директорот на дирекцијата доставува и дополнителен Извештај.

Извештајот содржи податоци кои се однесуваат на надлежностите на Дирекцијата² во врска со подготовка на законски и подзаконски решенија и текстови, развој на политики во областа на заштитата на лични податоци³, инспекциски надзор, ја цени законитоста на обработката (надзор) на лични податоци, води Централен регистар на збирки на лични податоци и претходно одобрување за обработка на лични податоци, издава забрани на натамошната обработка на лични податоци на контролори кои не ги почитуваат одредбите на Законот за заштита на лични податоци, одобрува пренос на лични податоци во странство, води прекршочна постапка⁴ за прекршоци предвидени во Законот и други работи. Дирекцијата е надлежна и за барања на надзорни тела во областа на заштитата на личните податоци на други држави во врска со извршувањето на нивните активности на територијата на Република Македонија.

¹ Основана е со Закон за заштита на личните податоци („Службен весник на Република Македонија“ бр.7/05, 103/08, 124/10 и 135/11), а Директорот на Дирекцијата го именува Собранието на РМ. На овој начин се обезбедува независност на институцијата во однос на органите на извршната, законодавната и судската власт, како и во однос на органите на локалната власт.

² Дирекцијата не е надлежна за исплата на паричен надомест за било какво кршење на Законот за заштита на личните податоци; не чува лични податоци; не може да спречи обработка на личните податоци, што се врши од страна на физичко лице, исклучиво заради лични активности или активности во домот; и Дирекцијата не е надлежна за обработката на личните податоци заради заштита на интересите на безбедноста и одбраната на Република Македонија или водење на кривична постапка не е во надлежност на Дирекцијата за заштита на личните податоци

³ Вклучително и меѓународна соработка во областа на заштитата на личните податоци и учество во работата на меѓународните организации и институции за заштита на личните податоци.

⁴ преку Комисија за одлучување по прекршок во согласност со закон

Дирекцијата ја управува Директор. Директорот го именува и разрешува Собранието на Република Македонија, во процедура која ја води Комисија за именување при Собрание на РМ, по пат на објава на јавен оглас, за период од 5 години со право на повторен избор, но не повеќе од двапати. Директорот има заменик кој го именува и разрешува Собранието, во процедура која ја води Комисија за именување при Собрание на РМ, по пат на објава на јавен оглас за период од 5 години. За својата работа директорот и неговиот заменик одговараат пред Собранието на РМ. Директорот раководи со администрацијата на Дирекцијата, организирана во повеќе сектори и одделенија⁵.

Работата на Дирекцијата во врска со нејзините „главни“ надлежности се остварува преку три сектора (Сектор за инспекциски надзор, Сектор за општи и правни работи и Сектор за европска интеграција, проекти и меѓународна соработка). Прашањата поврзани со заштита на личните податоци на социјалните мрежи и со „cloud computing“ се дел од работата на Секторот за инспекциски надзор и Секторот за општи и правни работи.

Секторот за инспекциски надзор преку пријави и по службена должност со теренски посети кај контролорите на лични податоци⁶ врши контрола на превземените мерки и активности за заштита на личните податоци. Во овој сектор непосредно инспекторите (Дирекцијата) се среќаваат со контролори кои користат услуги или се даватели на услуги во „облак“. Инспекцијата постапува односно врши инспекција во вид на редовен (според годишна програма и месечни планови), вонреден и контролен надзор. Може да постапува по барање/пријава од странка или *ex officio*.

Секторот за општи и правни работи во своето Одделение за нормативно-правни работи и постапување по предлози и претставки постапува во предметите кои се однесуваат на приватност на социјалните мрежи. Постапката по предмети кои се однесуваат на социјални мрежи Дирекцијата прима претставки поднесени на хартија, но и по електронски пат. Комуникацијата со странките (оштетен - заинтересирано лице - социјална мрежа -Дирекција) се одвива и преку личен контакт и по електронски пат.

⁵ (Анекс 1 - Органограм на ДЗЛП, Извор:

http://dzlp.mk/sites/default/files/Dokumenti/Organogram/ORGANOGRAM_DZLP.pdf)

⁶ А ако има потреба и кај обработувачите.

Оваа постапка е флексибилна и не толку формална во споредба со постапката за инспекциски надзор. Меѓутоа, зголемената активност на Дирекцијата и трендот на зголемување на претставки по оваа основа (*види Глава VI точка 1 од оваа Анализа*) веројатно ќе бара во иднина да се зголеми бројот на вработени кои ќе работат на овие предмети (со нови вработувања или прераспределба на задолженија, со определување замена/поддршка и сл.).

Дирекцијата исто така остварува меѓународна соработка на повеќе начини. Така, Дирекцијата е рамноправна членка со право на глас во Консултативниот Комитет (T-PD) на Советот на Европа на Конвенцијата за заштита на поединците во однос на автоматска обработка на личните податоци, Европската конференција за заштита на личните податоци (Пролетна Конференција), Конференцијата на Централно и Источно Европските органи за заштита на личните податоци, Работната Група за полиција и судство, Меѓународната Конференција на комесарите за заштита на личните податоци и приватноста, Меѓународната работна група за заштита на личните податоци во областа на телекомуникациите, case handling работилниците. Исто така, Дирекцијата има статус на набљудувач во Работната Група 29 на Европската Унија.

Покрај тоа, Дирекцијата има потпишано билатерални Декларации за соработка со 14 држави, претежно од Европа и регионот.

3. КОНТЕКСТ НА ИЗВЕШТАЈОТ

4. Статистички податоци⁷

Според истражувањата на Државниот Завод за статистика, бројот на интернет корисници во Македонија помеѓу домаќинствата/граѓаните, бизнис и јавниот сектор е во постојан пораст од 2006 година наваму од кога се започнати мерења во областа на Информатичкото општество⁸.

Во 2006 година 14% од домаќинствата/граѓаните имале пристап на интернет од дома⁹, додека во 2013 година 65,1% од домаќинствата/граѓаните имале пристап на интернет¹⁰. Од сите субјекти кои имаат пристап на интернет 80.3% се вклучуваат на интернет секој ден, а 92,7% се вклучуваат од дома. Од најразличните активности (*праќање/примање електронска пошта (e-mail); Учество во социјални мрежи; Читање on-line новини/весници/списанија; Барање информации поврзани со здравјето; Барање информации за образование, обука или курсеви; Наоѓање информации за производи/услуги; Симнување софтвер (се исклучиво софтвер за игри); Учење - следење на on-line курсеви; Учење - консултирање on-line енциклопедии; Барање работа или праќање молби; Учество на мрежи за професионалци; Користење услуги поврзани со патување и сместување; Продажба на производи/услуги (на пр.: преку аукции); Телефонирање преку интернет/видео повици преку web-cam; Интернет - банкарство*) поради кои субјектите се вклучуваат на интернет, најзастапено е присуството на социјалните мрежи со 84% од испитаниците, 69,6% праќање/примање електронска пошта (e-mail) и интернет телефонија или видео-фонија со 61%. Само 5,6% од испитаниците се користат со интернет од дома заради учество на мрежи за професионалци и 9,1% за интернет банкарство¹¹.

⁷ Превземени од истражувањата на Државниот завод за статистика на Р.Македонија.

⁸ Истражувањата се спроведуваат според методологијата и препораките на Евростат (Статистичко биро на Европската унија), во согласност со регулативите на Европската унија односно Регулативата на Европскиот парламент 808/2004.

⁹ <http://www.stat.gov.mk/pdf/2006/8.1.6.14.pdf>, последна посета ноември 2013.

¹⁰ <http://www.stat.gov.mk/pdf/2013/8.1.13.28.pdf>, последна посета ноември 2013.

¹¹ <http://www.stat.gov.mk/pdf/2013/8.1.13.28.pdf>, последна посета ноември 2013.

Во 2006 година 72,3% од деловните субјекти со над 10 вработени¹² имале пристап на интернет, додека во јануари 2013 година, широкопојасен пристап на интернет (преку фиксна или мобилна конекција) имале 91,5% од деловните субјекти со 10 или повеќе вработени¹³. Исклучок се деловните субјекти од финансискиот сектор каде 100% од референтните претпријатија користеле компјутери и интернет уште во 2006 година¹⁴. Во 2013 година исто така 7,4% од деловните субјекти за своите вработени обезбедиле далечински пристап до системот на е-пошта, документите или апликациите на претпријатието.

Во 2013 година¹⁵ првпат е измерена и употребата на **социјалните медиуми** кај деловните субјекти, како социјални мрежи, блогови, веб-страници за споделување на мултимедијална содржина (пр., Facebook, Twitter, YouTube, итн.), или wiki-алатки за споделување знаење. Социјални медиуми употребувале 36,2% од деловните субјекти¹⁶.

Во јавниот сектор во 2006 година пристап на интернет имале 100% од министерствата, 95,6% од државните агенции/организации, 94,4% од јавните претпријатија и 95,2% од органите на локалната самоуправа.¹⁷ За субјектите од јавниот сектор нема истражување за употреба на социјални мрежи или „*cloud computing*“ иако постојат, дизајнирани се и се нудат на граѓаните, бизнис секторот и сродните институции од јавниот сектор услуги кои се одвиваат on-line на сопствени Веб страници на институциите од јавниот сектор.

Нема мерења за користење на услуги на „*cloud computing*“ како посебна ставка, поради што не може да се добие јасна слика каков е обемот на користење на вакви сервиси во било кој од секторите (домаќинствата, бизнисот и јавниот сектор).

¹² Оваа категорија деловни субјекти според методологијата на Еуростат се зема како релевантна за споредба на податоците помеѓу ЕУ државите. Според методологијата на Еуростат постојат 4 категории на деловни субјекти од кои референтната е втора категорија.

¹³ <http://www.stat.gov.mk/pdf/2013/8.1.13.25.pdf> , последна посета ноември 2013.

¹⁴ <http://www.stat.gov.mk/pdf/2007/8.1.7.06.pdf> , последна посета ноември 2013.

¹⁵ Податоци кои всушност се однесуваат на 2012 година, а се обработени и објавени во известување од 2013 година.

¹⁶ <http://www.stat.gov.mk/pdf/2013/8.1.13.25.pdf> , последна посета ноември 2013.

¹⁷ <http://www.stat.gov.mk/pdf/2007/8.1.7.07.pdf> , последна посета ноември 2013.

5. Социјални мрежи

Социјалните мрежи преку интернет, или користењето на мрежни услуги за поврзување и општење со луѓе околу заеднички активности и интереси, може да биде одличен начин за остварување на интереси, воспоставување нови, и подобрување на постоечките пријателства, играње игри, и разменување на идеи. Издиференцирани се неколку категории на Веб сајтови – социјални мрежи:

*Социјални мрежи од генерален карактер*¹⁸- сервиси за социјално вмрежување во кои секој е слободен да се приклучи, а луѓето најчесто го презентираат својот реален идентитет па примарната употреба на сајтот е за интеракција со други лица преку профил-страници на интернет.

*Бизнис социјални мрежи*¹⁹ кои се разликуваат од оние со генерален карактер по тоа што се специјализирани за професионални контакти и за барање работа. На овие мрежи корисниците вообичаено ставаат на располагање повеќе професионални отколку лични податоци. Иако, и овие последните не се исклучени. Во оваа категорија би можел да се вброи и Twitter.

*Социјални мрежи за препорака на различни филмски и музички содржини*²⁰. Овие сајтови вообичаено имаат некои карактеристики како на оние од генерален карактер, но корисниците најчесто комуницираат меѓусебно на основа на заеднички интереси за музика, или филм отколку врз основа на општествени врски од реалниот свет.

*Мрежи за возобновување на врски меѓу луѓето (Reunion sites)*²¹ кои овозможуваат луѓето да бараат стари познаници од на пример училиште или војска. На овие мрежи профилите вообичаено не се одржуваат активно и многу често содржат само контакт информации. Но повторно, личните податоци не се исклучени.

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 и XING.

²⁰ Last.fm, Imeem, Flickster, и Buzznet.

²¹ Classmates.com и myLife (порано Reunion.com)

*Социјални мрежи за игри*²², кои на своите корисници им овозможуваат остварување на одредена активност. Некои овозможуваат играње, некои а пример информации за патувања и слично.

Социјални мрежи – *сајтови со посебни карактеристики за приватност*²³. Така има примери кои овозможуваат размена на животни искуства под псевдоними, социјални мрежи за деца со посебни родителски контроли и администрација на профили и слично.

Но што е социјална мрежа? Како развојот на социјалните мрежи влијае на приватноста?

Социјалната мрежа претставува форма на интеракција преку која луѓето прво воспоставуваат контакт со свои познаници, а потоа виртуелно остваруваат контакт и со нови лица со цел остварување на приватни или бизнис врски. Социјалната мрежа овозможува неограничена комуникација без потреба од физички контакт. Во кој обем ќе се остварува комуникацијата и интеракцијата ќе зависи од обемот на податоци кои корисникот ќе ги открие. При креирање на профилот (кориснички налог) корисникот мора да впише податоци за себе кои покрај тоа што се лични може да се и доверливи. Иако карактеристика на социјалните мрежи е дека корисникот сам бира (главно) кои податоци ќе ги остави па со тоа и влијае на сопствената безбедност на социјалните мрежи, често не се води сметка за овој аспект и несвесно корисниците се изложуваат на ризик.

Секако, не треба да се заборави и фактот дека кориснички профили отвораат и правни лица и тоа најчесто за цели на маркетинг и огласување преку што вредноста на одредена социјална мрежа расте. Колку е поголем бројот на корисници воопшто толку поголема е вредноста на мрежата. Од друга страна преку анализа на податоците на корисничките профили за потребите на одредена компанија се таргетираат оние корисници кои согласно анализите²⁴ би имале интерес за одреден производ или

²² Habbo, Gaia Online, CouchSurfing.

²³ Kaiyo, Experience Project, Imbee

²⁴ <http://www.coe.int/t/dghl/standardsetting/DataProtection/News/Web%20tacking.pdf>, последна посета ноември 2013.

услуга, кои се наоѓаат на местото каде што се нуди одреден производ или услуга²⁵ итн. Ова е значајно да се има предвид во контекст на заштита на приватноста и личните податоци вклучително и ризиците кои се поврзани со оваа сфера, а се опишани подолу.

Заштита на личните податоци е особено тешка кога станува збор за социјалните мрежи, бидејќи тие се базираат на објавување на податоци од страна на самите корисници. Така, меѓу потенцијалните ризици за квалитетна заштита на личните податоци се вклучени:

- *Случаи на phishing и pharming.* И двете појави се чести и се експлоатирани од страна на сајбер - криминалците со цел прибирање на лични или економски податоци на корисниците на интернет (кредитни картички, ПИН кодови , итн.)
- *Spat на социјалните мрежи.* Употреба на социјалните мрежи, како платформи за испраќање несакани пораки.
- *Неовластено индексирање* од страна на интернет пребарувачите.
- *Неконтролиран пристап до профили.* На повеќето социјални мрежи може да се објават податоците на корисничкиот профил целосно или делумно, по што секој може да пристапи до личните информации без изрична согласност на сопственикот.
- *Напаѓачки софтвери или Malware* кој е всушност вид на компјутерска програма која самата се инсталира на корисничкиот компјутер без знаење на корисникот. Програмата е направена да собира осетливи информации кои се зачувани на корисничкиот компјутер, како што се банкарска лозинка за работење преку Интернет или детали од кредитна картичка. Потоа ја користи Интернет конекцијата на корисникот за да ги испрати овие податоци до криминалци кои ги користат за незаконско дејствување.

²⁵ Во денешно време употребата на преносни компјутери, паметни телефони и други направи несвесно придонесува кон овој тренда на анализа на корисничките профили, а со тоа и задирање во сферата на личните податоци.

- *Кражба на идентитет.* Се почесто се случува корисник да идентификува постоење на нов/двоен идентитет во дигитален формат зависно од тоа дали прв пат се обидува да направи регистрација на профил или веќе поседува таков. Во крајна линија некој друг го користи неговиот/нејзиниот идентитет, а не тој самиот/самата.
- *Контекстуализирано рекламирање.* Некои сервиси (како: Google ads) се базираат на преференции на корисникот при посета на одредени сајтови или преку читање на некоја содржина (иако преференциите не се експлицитно или свесно поставени од корисникот, тие се резултат на историјата на пребарување, прегледување страници и историја на кликање на огласи) и се обидуваат да понудат огласи кои одговараат на содржината од историјата на пребарување. Ваквите практики може да се сметаат за неприфатливи во поглед на прашањето за приватност.
- *Инсталација и употреба на "колачиња" без согласност на корисникот на социјалната мрежа.* Имено, постои можност веб страната да користи *cookies* со што си овозможува услови за следење на активностите на своите корисници. Благодарение на овие алатки, социјалните мрежи може да го регистрираат местото од каде што корисникот е поврзан, времето на поврзување, уредот од кој тој / таа пристапил на платформа (фиксни или мобилни уреди), оперативниот систем кој тој / таа го користи, најпосетените страници во рамките на еден веб-сајт, бројот на направени кликови, и многу други податоци кои всушност откриваат детали во врска со животот, интересите, потребите и слично на корисникот во мрежата.
- *Злоупотреба* - Кога личните податоци на Интернет се јавно достапни, луѓето можат да ги искористат и да изнајдат начини да ги злоупотребуваат или да му се закануваат на сопственикот на податоците. Тие луѓе можат да му бидат познати или непознати на корисникот, па зголемено внимание е неопходно.
 - *Злоупотребата може да се рефлектира на пример во врска со дигиталните отпечатоци (технологија која вклучува алгоритам кој*

ги анализира огромниот број на технички карактеристики и подесувања за да се генерира единствен идентификатор за идентификација на специфичен компјутер) бидејќи повеќе во Европа и помалку во САД, IP адресата може да се смета за „личен податок“, конкретни дигитални отпечатоци може да се поврзат со определени индивидуи, машинските дигитални отпечатоци може да се комбинираат со други посензитивни информации за да се креираат профили и да се вмрежат податоците за да се дознае повеќе за одредено лице, и слично.

- *Plug-ins на социјалните мрежи се апликации кои овозможуваат лесно споделување на содржини, преференции и сл. Приватноста во врска со овие апликации може да биде загрозна од самиот корисник за сопствената приватност (поради несвесност за последиците од откривање на лични податоци преку користење на plug-ins), корисник кон корисник (намерно или ненамерно) каде што на пример означување на некое лице на фотографија може да овозможи пристап до содржината на истата и на трети лица кои инаку не се поврзани со лицето на фотографијата; повреда на приватноста со апликација - кога корисникот користи апликација развиена од трето лице, а која користи поинаква шема за безбедност на приватноста (функционалности и трансмисијска политика на апликацијата) од онаа на социјалната мрежа; повреда на приватноста од старана на социјалната мрежа во ситуација кога не постои можност за споредба на опциите за приватност пред и по нивната промена, вклучително и функционалните и трансмисијски аспекти на plug-in от на мрежата.*
- *Условите за користење тешко се разбирливи. Многу социјални мрежи објавуваат лошо напишани услови на користење кои може повеќе да збунат отколку да разјаснат. Често се оградуваат од одговорност, а условите може да се сменат и без да се известат корисниците. Секако важно е и прашањето кој ги поседува податоците откако мрежата би престанала да постои?*

- *Употреба на лични податоци за да се оформат детални профили на поединци.* Facebook и Google се најпознатите бизниси кои систематски прибираат податоци за да подоцна продаваат целно рекламирање кое се базира на профили (види контекстуализирано рекламирање). Постојните трендови на Big Data се состојат во нови можности за компаниите кои истовремено го зголемуваат ризикот врз приватноста.

Македонија

Социјалните мрежи во подлабока смисла се користат и за други цели освен за нивната првична намена. Така се интензивира трендот на користење на овие мрежи од страна на компаниите за поактивна комуникација со клиентите, личен маркетинг и претворање на вработените во „brand ambassadors“²⁶, што претставува реалност и во Р. Македонија. Меѓутоа, не е забележана активност на Дирекцијата во овој правец. Со оглед дека тренд на дистрибуција на бизнис информации низ приватни социјални мрежи е реалност, бизнисот би требало да обрне посебно внимание на овој начин на активности и заштита на личните податоци до кои доаѓаат во допир од можна злоупотреба. Воедно, се отвора ново поле за активности на Дирекцијата како надлежна за заштита на правото на приватност.

Државниот Завод за статистика согласно методологијата за статистички истражувања на Eurostat го истражува прашањето на социјалните мрежи и нивната употреба од страна на граѓаните, бизнисот и јавниот сектор во квантитативна смисла што е презентирано погоре.

Во Р. Македонија се регистрирани речиси 1.000.000 профили само на Facebook²⁷ односно оваа социјална мрежа ја користат 48% од населението (од кои 92% ја користат активно). Според истражување спроведено со интернет анкета врз примерок од 800 испитаници (корисници на Facebook) од страна на рејтинг Агенција просечен корисник

²⁶ https://www.taylorwessing.com/globaldatahub/article_social_media_enterprise.html, последна посета ноември 2013.

²⁷ <http://www.slobodnaevropa.org/content/na-balkanu-facebook-koriste-najvise-u-srbiji-/24909738.html>, последна посета декември 2013.

на оваа мрежа поминува логиран на мрежата повеќе од 3 часа дневно.²⁸ Оттука, веројатноста за ризици е многу голема. Според споменатото истражување корисниците на мрежата сè уште не премногу активно се поврзуваат со брендови, но активностите на бизнисот во смисла на маркетинг на социјални мрежи не е занемарлив. Исто така, за очекување е дека активностите на бизнисот на социјалните мрежи веројатно во иднина само ќе се интензивираат па со тоа и прашањето за безбедноста на личните податоци ќе биде се поактуелно.

6. Cloud computing

Тоа е главна ИКТ тема во последните неколку години: *cloud computing*. Денес, секој е поврзан на интернет и голема е веројатноста дека на некој начин работи во "облакот". Преку ажурирање на вашиот профил на Фејсбук, користење апликација за онлајн канцеларија или качувањето датотеки на онлајн сервис за складирање се начините на користење на „облак“. Cloud computing е значаен фактор за современите бизниси, бидејќи со користење на услуги во „облак“ може драстично да се намалат трошоците на работење. Овој концепт им дава и на мали (start-up) компании можност да влезат на големите пазари без високи, ризични start-up трошоци. Значењето на cloud computing само ќе се зголеми во иднина; Меѓународната корпорација за податоци (IDC²⁹) предвидува дека 80% од новите комерцијални корпоративски апликации ќе бидат распоредени на „облак“ платформи па со право може да се тврди дека cloud computing услугите се од суштинско значење за интернетот каков што го познаваме.

²⁸ <http://it.com.mk/koj-e-prosechniot-makedonski-korisnik-na-facebook/>, последна посета октомври 2013.

²⁹ <http://www.idc.com/>, последна посета октомври 2013.

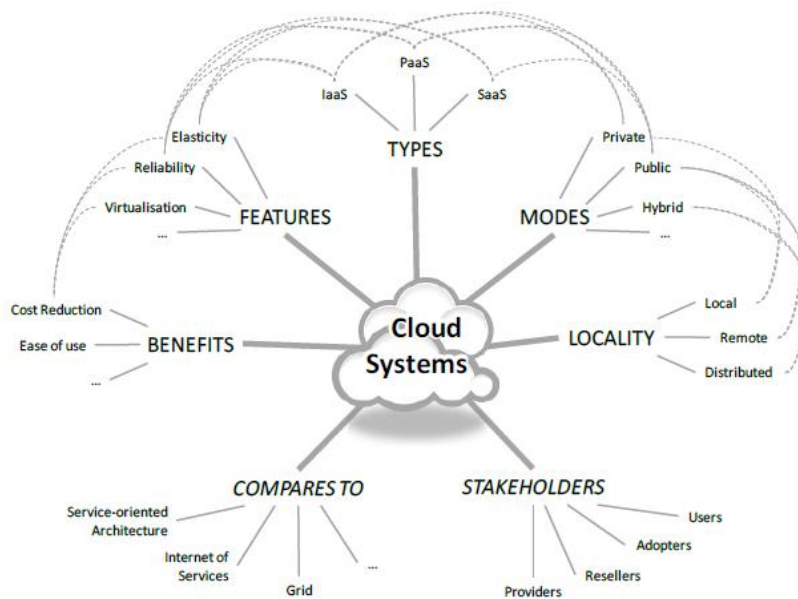


FIGURE 1: NON-EXHAUSTIVE VIEW ON THE MAIN ASPECTS FORMING A CLOUD SYSTEM

Наслов на Фигурата: Неконечен преглед на главните аспекти кои го формираат системот на „облак“.

Извор за Фигура 1: <http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf> , како експертите гледаат на “Cloud computing” во извештајот насловен како „Иднината на Cloud computing – Можностите на Европскиот Cloud computing по 2010“ (The future of cloud computing opportunities for European Cloud Computing beyond 2010),

Глобален лидер на услуги се американски провајдери на услуги, па во одговор на таквата состојба Европа развива нова стратегија за “Cloud computing” која ќе го олесни работењето на бизнисот, а ќе ја зацврсти заштитата на личните податоци³⁰. Пристапот е дека Пан-европски Cloud computing сервис може да биде одговор на доминацијата од преку Атлантикот.

“Cloud computing” е модел кој овозможува сеприсутен, удобен, мрежен пристап „на барање“ до достапни компјутерски ресурси кои може соодветно да се конфигурираат (на пример, мрежи, сервери, складирање (storage), апликации и услуги) кои можат да бидат брзо овозможени и дадени на употреба со минимален напор за нивно управување или интеракција со добавувачот на услугата. Овој модел на Облак се

³⁰ <https://ec.europa.eu/digital-agenda/en/pillar-vii-ict-enabled-benefits-eu-society/action-109-develop-and-implement-public-service> , последна посета декември 2013.

состои од 5 основни карактеристики, 3 сервисни модели и 4 модели на распоредување³¹“.

	Управувано од	Сопственик на инфраструктура	Овозможен хардвер
Јавен	CSP (Провајдер на облак услуги)	CSP (Провајдер на облак услуги)	НЕ
Приватен, екстерен	CSP (Провајдер на облак услуги)	CSP (Провајдер на облак услуги)	ДА
Приватен, интерен	Интерна организација	Интерна организација	ДА
Хибриден	Мешана	Мешана	CSP (Провајдер на облак услуги)

Табела 1 – Класификација на типови „Облак“³²

Главни карактеристики, но листата не е исцрпена:

1. *Сервис по потреба* (On-demand self-service). - Корисникот може самостојно без интеракција со човек од страна на испорачателите на услуги може да користи различни ИТ капацитети.
2. *Широк мрежен пристап* (Broad network access). - Капацитетите се достапни преку мрежа и преку употреба на различни клиентски платформи (компјутери, мобилни телефони, таблети итн.)
3. *Достапност на ресурси* (Resource pooling). – Ресурсите (физички и виртуални ресурси) на провајдерот на компјутерски ресурси се достапни за повеќе корисници одеднаш со различни потреби, кои се прават достапни и се врши редистрибуција според тие потреби. Во принцип корисникот нема увид или контрола над точната локација на ресурсите кои ги користи, но е определиво каде би можеле да се наоѓаат (на пример: држава, регион, податочен центар).
4. *Огромна еластичност на услугите* – обемот на услуги кои се користат во облак може нагло да се зголемуваат и/или намалуваат во зависност од обемот на побарувачката. За корисникот најчесто се чини дека можностите се неограничени и дека ќе одговараат на неговите потреби во било кое време.

³¹ <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf> , дефиниција на Националниот Институт на стандарди и технологии (The National Institute of Standards and Technology (NIST)) кој подготвува стандарди за употреба во федералните американски агенции, Септември 2011.

³² Меѓународно прифатена типологија. Вклучително и стандардите на НИТС.

5. *Мерливи услуги* – системите кои овозможуваат услуги во облак автоматски обезбедуваат информации за нивото на искористеност на услугите. Искористеноста може да се мери, контролира и да се извести и давателот на услугата и корисникот за тоа.

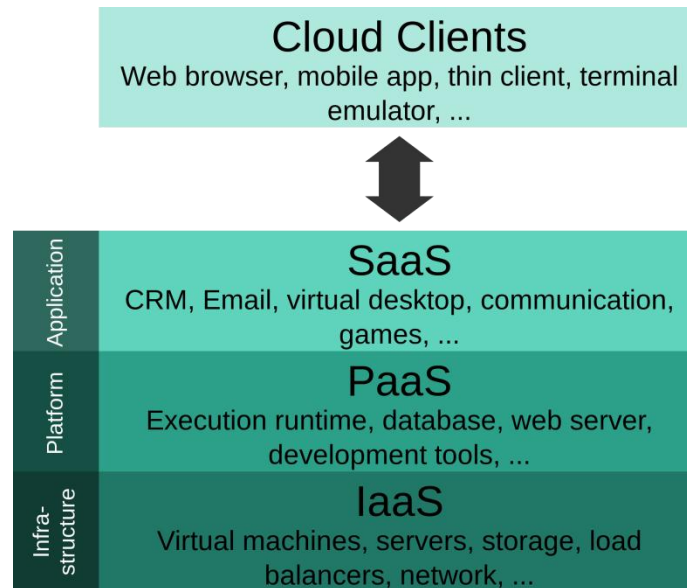
Модели на услуги:

Познати се три основни модели на услуги во „облак“ (иако може да се пропознаат и други) кои се помалку или повеќе дефинирани на сличен начин, но во основа значат следно:

- *Софтвер како услуга* (Software as a Service (SaaS)). – Ова е модел во кој преку дистрибуција на софтвер кој е хостиран од давателот на услугата и кој е достапен во вид на апликации за корисникот на услугата преку мрежа, најчесто преку Интернет. Корисникот нема влијание/контрола врз инфраструктурата која ја користи, вклучително и на мрежата, серверите, оперативните системи, складиштето или карактеристиките на апликациите, освен по исклучок.
- *Платформа како услуга* (Platform as a Service (PaaS) – Корисникот самостојно може да креира апликации со помош на алатки и ресурси како што се програмски јазици, библиотеки, услуги и различни алатки, но не ја управува и нема контрола врз оперативните системи, складиштето. Тој може да има влијание врз карактеристиките на апликациите, но нема контрола над ИТ инфраструктурата која се користи во облакот.
- *Инфраструктура како сервис* (Infrastructure as a Service (IaaS)³³ - Корисникот користи хардверски ресурси (за процесирање на податоци, складирање, вмрежување и друго) на кои може самостојно да инсталира и да користи компјутерски програми и апликации. Тоа е вообичаено стандардизирана понуда која провајдерот на ваква услуга ја нуди на корисниците „на барање“. Корисниците можат самостојно да постават сопствен Веб базиран интерфејс кој има улога на ИТ конзола за

³³ Nicholas Carr, автор на статијата „Дали е важно?“ прв во 2006 година го употребил терминот „Хардвер како сервис“/“Hardware as a Service” за да ги опише сервисите како што е на пример облакот на Amazon на Amazon.com - Elastic Compute Cloud (EC2). Овој поим е претходница на IaaS терминот.

управување. И кај оваа услуга корисникот нема контрола над ИТ инфраструктурата.



Автор на графикон: Bikeborg

Во литературата се посочува дека секој од овие три модели на услуга носи елемент кој е заеднички за сите, а тоа е виртуализација. Па така се објаснува дека IaaS е виртуализација на сервери, складирање и мрежи, PaaS е (во некоја рака) е виртуализација на комбинација на услуги IaaS и SaaS. На крај SaaS е виртуализација на нивото на апликации преку користење на мета - податоци.

Модели на имплементација:

Услугите во облак може да се имплементираат на неколку начини кои во продолжение се кратко образложени.

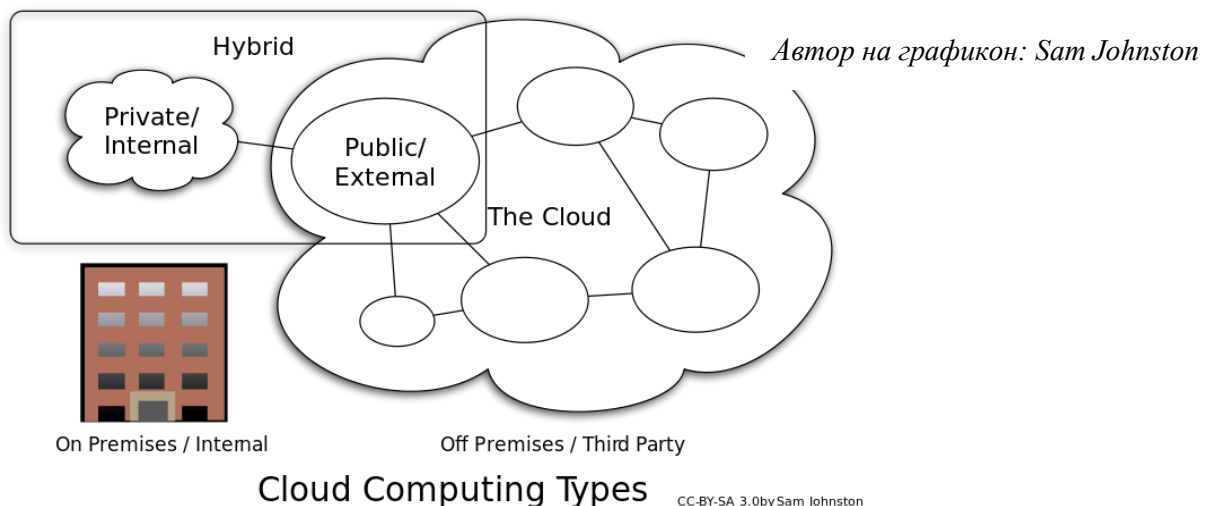
Приватен облак – Инфраструктурата на облакот е целосно посветена на еден корисник (кој може да ја поседува, да користи туѓа или да комбинира сопствена и туѓа, да ја има во своите простории или надвор од нив) или е целосно обезбедена негова изолација од други корисници.

Заеднички облак – се однесува на инфраструктура на облак која се дели помеѓу организации, членови на некоја заедница, вработени и слично кои вообичаено имаат заеднички барања за безбедност, приватност, функционалност и соодветност. Може да биде управувана ваквата структура од една или повеќе организации или трета

страна односно комбинација од нив. Инфраструктурата, како и во претходниот случај, може да биде сместена во просториите на корисниците или надвор од нив.

Јавен облак – Се дефинира како флексибилни и еластични капацитети кои им се нудат на надворешни корисници преку користење на интернет технологии. Овој тип на облак е од отворен тип и е наменет за употреба на широката јавност. Користењето на јавен облак генерира економија од обем и заедничко користење на исти ресурси што во крајна линија води до намалување на трошоци и зголемување на изборот на технологии кои ќе се користат за потребните услуги. Во јавниот облак сите имаат еднаков третман во користењето на ресурсите (би можеле да ги користат и јавни и приватни институции од различни институции во исто време) и поради тоа не може да се гарантира точно каде ќе бидат лоцирани и зачувани податоците за кои се користи услугата. Може да биде ваквата структура управувана од бизнис субјект, академски субјект, владина институција или комбинација од нив.

Хибриден облак – тоа е збир од некој од горните модели на имплементација кои и натаму остануваат самостојни но поради некоја причина се меѓусебно обврзани да комуницираат. Причина за тоа може да биде примена на некој стандард, примена на технологија итн.



Македонија

Она што е важно да се потенцира во моментот е дека во пракса постојат одредени состојби или појави кои се уште не се перципираат како “Cloud computing“, а кај кои *de facto* е важно прашањето за заштита од злоупотреба на лични податоци.

Така, во подем е нов вид на on-line услуги на бизнис секторот – продажба на интернет³⁴, иако пракса на купување на интернет постои поодамна. Од перспектива на заштитата на лични податоци е важно следното. Според податоците на интернационалниот картичен систем, во 2011 година во Македонија се направени 77.000 трансакции во електронска трговија, додека за 2013 година се очекува таа бројка да биде 265.000 трансакции³⁵. Од 2007 година регистрирани се 300 компании во Македонија кои продаваат стоки и услуги на интернет. За успешна реализација на on-line парични трансакции во реално време кои понекогаш може да бидат покренати истовремено од повеќе корисници кон еден добавувач, а за кои е потребна брза проверка на податоци за да се комплетира трансакцијата во крајна линија значи ангажирање на обемен ИТ потенцијал. Во таква ситуација решението е “Cloud computing”³⁶. Оттука, потребно е да се посвети внимание на овој тренд.

Исто така, во светски рамки се познати појави на воспоставување системи за пријава на прекршоци и случаи на корупција (*Whistleblowing*) во рамки на организациите. Многу често овие системи се воспоставуваат on-line, па се третираат како системи во облак. Бидејќи пријавувачи се физички лица автоматски се доведува во прашање заштитата на приватноста и личните податоци како такви. Во рамки на оваа Анализа не се правени детални истражувања на оваа тема но во државата постојат некои општо познати сервиси за пријава на корупција³⁷. Ваквите системи во Шведска на пример се во надлежност на органот за заштита на лични податоци кој во случај друга организација која не е државен орган на кој со закон му е дозволено да воведат систем за пријави, посака да воведат ваков систем, им издава дозвола за примена на системот³⁸. Важна е заштитата на приватноста и движењето на податоците во околина која не се третира дека по default е ослободена од ризици за злоупотреба на личните податоци.

³⁴ http://www.kanal5.com.mk/vesti_detail.asp?ID=27621 , последна посета 9 јануари 2014.

³⁵ Не се достапни нови анализи во времето на пишување на овој Извештај.

³⁶ На пример Амазон користи “Cloud computing” за да ја обавува својата дејност.

³⁷ На пример на Веб страната на <http://www.transparency-watch.org/reports/submit> може да се поднесе пријава за корупција, но нема доказ дали и како се воспоставени правила и спроведени мерки за заштита на лични податоци.

³⁸ <http://www.datainspektionen.se/Documents/vagledning-whistleblowing-eng.pdf>, последна посета декември 2013.

7. ПРАВНА РАМКА

8. Национална правна рамка

За целите на оваа Анализа консултирани се во поголема или помала мерка прописите споменати подолу.

Правото на заштита на личните податоци е регулирано со член 18 од Уставот, кој ги поставува темелите за гарантирање на безбедноста и тајноста на личните податоци и заштита од повреди на личниот интегритет на граѓаните.

Детално сферата на заштитата на личните податоци е регулирана со следните прописи:

Закони

1. Закон за заштита на личните податоци („Службен весник на Република Македонија“ бр. 7/05, 103/08, 124/10, 135/11)
2. Закон за ратификација на Дополнителниот Протокол кон Конвенцијата за заштита на поединците во поглед на автоматската обработка на лични податоци, во врска со надзорните тела и преку - граничен пренос („Службен весник на Република Македонија“ бр. 103/08)
3. Закон за ратификација на Конвенцијата за заштита на лица во однос на автоматска обработка на податоци („Службен весник на Република Македонија“ бр. 7/05)
4. Секторски закони од повеќе области (електронски комуникации, образование, здравство, нотаријат, обезбедување имоти и лица, туризам, трговија, банкарство, итн.).

Правилници и упатства

1. Правилник за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци - пречистен текст ("Службен весник на Република Македонија" бр.38/09 и 158/10)
2. Правилник за формата и содржината на образецот на Известувањето за обработка на личните податоци и за начинот на известувањето во Централниот регистар на збирки на лични податоци - пречистен текст ("Службен весник на Република Македонија" бр. 155/08)
3. Правилник за содржината и формата на актот за начинот на вршење на видео надзор („Службен весник на Република Македонија“ бр. 158/10)

4. Правилник за формата и содржината на образецот за евиденција на извршениот пренос на лични податоци („Службен весник на Република Македонија“ бр. 158/10)
5. Правилник за начинот на вршење на инспекцискиот надзор („Службен весник на Република Македонија“ бр. 158/10)
6. Правилник за формата и содржината на поканата за едукација, начинот на спроведување на едукацијата, како и начинот на водење („Службен весник на Република Македонија“ бр. 158/10)
7. Правилник за начинот на водење на единствена евиденција на прекршоците, изречените санкции и донесените одлуки во прекршочна постапка, како и начинот на пристап до информации кои се содржани во евиденцијата („Службен весник на Република Македонија“ бр. 136/08)
8. Правилник за образецот, формата и содржината на легитимацијата и за начинот на нејзиното издавање и одземање - пречистен текст ("Службен весник на Република Македонија" бр. 143/08) [Преземи]
9. Правилник за формата и содржината на барањето за утврдување на повреда на правото на заштита на личните податоци („Службен весник на Република Македонија“ бр. 144/11)
10. Упатство за начинот на вршење на надворешна контрола – Акт на Дирекцијата
11. Упатство за дополнување на упатството за начинот на вршење на надворешна контрола – Акт на дирекцијата
12. Извештај од извршена (внатрешна или надворешна) контрола на информацискиот систем и информатичката инфраструктура - образец , Акт на Дирекцијата

Во врска со социјалните мрежи и „cloud computing“ применливи се општите прописи за заштита на личните податоци, а во секој поединечен случај е потребно да се провери применливоста и на секторскиот закон.

Од анализата произлегоа општи препораки за измени во правната рамка кои се посочени во делот на Заклучоци и препораки.

9. Меѓународна правна рамка

Дополнително покрај Законот за заштита на личните податоци, правната рамка за заштита на личните податоци во Р. Македонија ја вклучува Европската конвенција за човекови права и Конвенцијата на Советот на Европа No.108/1981 за заштита на

поединци, која се однесува на автоматски заштита на личните податоци, како и дополнителниот Протокол кон оваа Конвенција за надзорните органи и прекугранични пренос на податоци кои се ратификувани од страна на Парламентот на државата.

Националното законодавство е исто така хармонизирано со Европското (Директивата 95/46/ЕС на Европскиот Парламент и на Советот за заштита поединците во однос на обработката на личните податоци и на слободниот проток на таквите податоци) во рамки на процесот на пристапување на државата кон ЕУ³⁹. Во таа смисла Дирекцијата и легислативно и во пракса ги применува новините во врска со заштитата на лични податоци и активно учествува во процесот на дефинирање на нови трендови за поефикасна заштита.

Целосно се следат новините во Европа од причина што правилата кои се предлагаат ќе треба да се имплементираат и во националното законодавство. Така се има во предвид предлогот да се подигне нивото на регулација од Директива на ниво на Регулација со која ќе се постигне хоризонтална усогласеност на правилата за заштита на лични податоци во контекст на новите технологии и која ќе биде применлива на Компаниите во Унијата, но и за оние кои нудат стоки и услуги на граѓаните на Европа, особено во on-line контекст.

Предлозите да се зголеми одговорноста на контролорите и обработувачите воопшто, како и преку вклучување на нови барања предложени со новата Регулација вклучително изработка на документација за обработка на податоци, подготовка на оценки за влијание на приватноста, приватност по default (privacy – by - design/default), и споделена одговорност на обработувачите на податоци се новини за кои ќе биде потребно да се инкорпорираат во националното законодавство. Ова важи за другите аспекти на регулативата кои може да предизвикаат контекстуални промени. Секако, ако Регулацијата биде усвоена на начин како е и предложена.⁴⁰

³⁹ http://ec.europa.eu/justice/data-protection/law/index_en.htm, последна посета декември 2013.

⁴⁰ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52012PC0011:en:NOT> , последна посета декември 2013.

Во предвид се има и предлогот на новата директива за Сајбер безбедност⁴¹. Предлозите за воведување обврски за организациите да воведат технички и организациски мерки, обврска да спроведат безбедносна ревизија и обврска да пријавуваат повреди кон регулаторот се новини кои дополнително ќе предизвикаат контекстуални промени. Особено поради предлогот оваа директива да се применува на организации како што се: комерцијални (трговски) платформи, плаќања преку интернет, социјални мрежи, пребарувачи на интернет, Cloud computing сервиси, продавници за софтверски апликации, снабдувачи со енергија, компании за транспорт/логистика, кредитни институции и берзи, организации од областа на здравството.

Заради одржување чекор со трендовите во Европа важно е и следење на стратешките определби на Европската комисија (ЕУ Стратегија за заштита на лични податоци) во оваа сфера и тоа: 1) поедноставување на стандардите и сертификацијата за cloud computing, 2) развивање на нови модел договори и клаузули, и 3) покренувањето иницијатива за European Cloud Partnership.

10. МЕТОДОЛОГИЈА

За изработка на извештајот се користени традиционални истражувачки методи кои опфаќаат анализа на примарни и секундарни правни и други извори (на пример: националното и ЕУ законодавство, официјални стратешки документи и пракса). За да се добие поконкретна слика за трендовите на полето на интерес на оваа анализа употребени се и други извори на информации (Веб страници, блогови и други модерни формати) во обем кој овозможува формирање релевантни заклучоци.

За проценка на состојбата во Дирекцијата и подготвеноста на персоналот да се справи со темите на приватност на социјалните мрежи и во Cloud computing спроведено е

⁴¹ <http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security>, последна посета декември 2013.

истражување преку прашалник за вработените во Дирекцијата⁴², како и интервјуа со релевантни вработени.

Ставови и дефиниции на институции како НИСТ и експертската група на Европската комисија кои се однесуваат на приватност, социјални мрежи и Cloud computing се исто така земени предвид и соодветно потенцирани во текстот на Анализата. Земени се предвид каде е релевантно и академски извори.

Во ограничен обем консултирани се и технички извори (веб страни и сервиси на технички компании како што се Оракле, Хјулит Пакард, Микрософт, Фасебук итн) кои се популарни во моментот.

Во врска со правната рамка консултирани се прописите од глава IV, точка 1 и точка 2, па така покрај Законот за заштита на лични податоци и секторските закони, како и подзаконската регулатива, консултирани се и Директивата за заштита на лични податоци заедно со Анализа на усогласеноста на Законот со Директивата, предлогот на Регулацијата за заштита на лични податоци и друга документација. Земени се предвид и мислењето на Работната група од чл.29, документацијата на Супервизорот за заштита на лични податоци, ставовите на Берлинската група и други. Консултирана е и релевантната пракса на ЕСП (European Court of Justice) иако директно не е употребена во самата анализа. Таа во контекст на темата со која се занимава овој Проект може да се употреби за придружна документација (прирачници, водичи и сл.) која треба да се подготви за потребите на Дирекцијата.

Секако во заклучок, се употребено за овој Извештај е анализирано само од перспектива на заштита на личните податоци на социјалните мрежи и „Cloud computing“.

11. АНАЛИЗА НА СОСТОЈБАТА

Дирекцијата постапува во предмети кои се поврзани со социјалните мрежи и „Cloud computing“.

⁴² Прашалникот послужи за анализа на емпириски податоци во рамки на подготвување на овој Извештај.

Преку Одделението за претставки и поплаки, граѓаните можат да поднесат барање за заштита на нивната приватност. Доколку барањето е релевантно, а Дирекцијата надлежна службеникот комуницира со соодветната социјална мрежа. Најголем успех е забележлив со социјалната мрежа Facebook со која се остварува неформална соработка. Иако соработката се одвива добро, непостоењето на формален документ за соработка (меморандум на пример) може да се третира за недостаток. Ова се однесува особено на другите социјални мрежи со кои Дирекцијата се обидела да оствари соработка, но во пракса се покажало дека провајдерот не покажува интерес да го стори тоа.

Овие податоци се споредени со состојбата во Норвешка и може да се заклучи дека нема разлика во врска со можностите за комуникација и соработка со социјалните мрежи кои им стојат на располагање на институциите за заштита на лични податоци.

12. Претставки до Дирекцијата

Во 2013 година во периодот од 01.01.2013 до 31.12.2013 година до Дирекцијата се поднесени вкупно 404 претставки од граѓани и правни лица по сите основи. Дел од овие претставки се однесуваат на злоупотреби на социјалните мрежи. Дирекцијата постапува и по овие претставки. Во 2013 година процесирани се вкупно 252 предмети по претставки во врска со злоупотреба на личните податоци на социјалните мрежи. Дирекцијата главно процесира предмети кои се однесуваат на најчестите видови на злоупотреби на социјалните мрежи како што се пријави за бришење на лажни профили на Facebook (187/252), бришење на хакирани профили (43/252). Дирекцијата постапувала и по претставки за откривање на ИП адреса, неовластено објавување на фотографии, претставки поради злоупотреба на податоци за малолетници и други. Од 252 претставки за наведениот период вкупно 218 се однесувале на злоупотреби на социјалната мрежа Facebook. Во споредба со минатите години видлив е тренд на зголемување на бројот на претставки кои се однесуваат на овој вид злоупотреби. Поради зголемената активност на Дирекцијата за јакнење на јавната свест за можните злоупотреби на личните податоци на социјалните мрежи, за очекување е ваков нагорен тренд. Тој секако треба да се очекува дека и во иднина ќе има раст, имајќи ги

предвид стратешките определби на Дирекцијата за интензивирање на активностите во оваа сфера.

Во контекст на оваа констатација во продолжение се наведени неколку статистички податоци за бројот на претставки односно предмети по кои постапувала Дирекцијата во изминатите години. Така, за илустрација во 2012 година во периодот од 01.01.2012 - 31.12.2012 година во Дирекцијата се примени вкупно 385 претставки од кои 207 се претставки за злоупотреби на личните податоци на социјалните мрежи.⁴³ Во врска со злоупотребата на личните податоци на социјалните мрежи, за бришење на лажен профил на Facebook поднесени се 118 барања, за пробиено корисничко име или лозинка на профил на Facebook поднесени се 49 барања, за отстранување на видеа и фотографии од You Tube поднесени се 9 барања и 31 други видови на барања (бришење на е-маил адреси, препратени предмети за постапување од Министерството за внатрешни работи и друг и видови на злоупотреби на социјалните мрежи и прашања).⁴⁴

Во периодот од 01.01.2011 година до 31.12.2011 во Дирекцијата примени се 363 претставки. Претставките се од областа на личните податоци, при што, од вкупно 363 претставки, 127 се претставки за злоупотреби на личните податоци на социјалните мрежи.⁴⁵ Во врска со злоупотреби на личните податоци на социјалните мрежи, за бришење на лажен профил на Facebook се поднесени 87 барања, за пробиен профил 12 барања, за злоупотреба на лични податоци од група на Facebook поднесени се три барања, за You Tube три барања и 11 други видови на барања, бришење на е-маил адреси, препратени предмети за постапување од Министерството за внатрешни работи и други видови на злоупотреби на социјалните мрежи и прашања.⁴⁶

Традиционално физичките лица се тие што поднесуваат повеќе претставки од правните лица и тој сооднос е приближно 10 (физички) : 1 (правни лица).

⁴³ Извештај за работењето на дирекцијата за заштита на личните податоци во 2012 година.

⁴⁴ Извештај за работењето на дирекцијата за заштита на личните податоци во 2012 година.

⁴⁵ Извештај за работењето на дирекцијата за заштита на личните податоци во 2011 година

⁴⁶ Извештај за работењето на дирекцијата за заштита на личните податоци во 2011 година.

Советување

Дирекцијата преку своите активности односно во комуникацијата со лицата кои поднеле претставки поради злоупотреби на социјалните мрежи покрај спроведување на постапка за поддршка на засегнатите лица, истовремено дејствува и советодавно. Исто така, преку реализација на Комуникациската стратегија и различните форми на соработка со други институции и невладиниот сектор дополнително на општо ниво ја информира јавноста и на теми кои се однесуваат на социјалните мрежи. Но, пожелно е советодавната улога на Дирекцијата дополнително да се изгради понатаму, па во тој контекст и да се востанови (Веб) платформа преку која оваа улога на Дирекцијата и ќе се остварува.

13. Инспекциски надзор

Согласно Законот за заштита на личните податоци, Законот за општата управна постапка, Правилник за технички и организациски мерки за обезбедување тајност на обработката на личните податоци, Правилник за инспекциски надзор, секторска легислатива која се однесува на соодветниот контролор на лични податоци кај кој се врши надзор, но и Мислењето 05/2012 за *Cloud computing* од јули 2012 и Работниот документ за „*Cloud computing*“ – Приватност и прашања за заштита на податоци „Сопот Меморандум“ од април 2012⁴⁷ Дирекцијата спроведува преку Секторот за инспекциски надзор (види Глава II од оваа Анализа) инспекција кај контролорите на лични податоци. Инспекцискиот надзор го вршат овластени инспектори кои се вработени во Дирекцијата. Тие вршат три вида надзор: редовен, вонреден и контролен надзор.

Редовниот надзор се врши врз основа на годишна програма за инспекциски надзор, а се реализира преку месечни оперативни планови за инспекциски надзор во кои се прецизирани контролорите, збирките што се инспектираат и датата на отпочнување на инспекциските надзори.

Постапката за редовен надзор почнува со испраќање Известување за редовен инспекциски надзор до контролорот на лични податоци. Во Известувањето се

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

информира контролорот за денот кога инспекторот ќе направи посета, ќе му се укаже на обврската пред денот на закажаниот надзор да достави пополнета Основна листа за проверка⁴⁸ која е објавена на Веб страната на Дирекцијата. Листата содржи 28 прашања групирани во две точки (1. Прашања за контролорите и 2. Прашања за збирките). Информациите содржани во оваа листа се основа за спроведување на надзорот на терен, за кој инспекторот детално се подготвува. Пред да ја реализира посетата на терен проверува дали се исполнети формалните барања поставени во регулативата согласно која се спроведува надзорот и тоа во врска со постапката за надзор, законските барања кои се однесуваат на контролорите на лични податоци и збирки и слично (на пример: дали контролорот благовремено го примил Известувањето за надзор, дали благовремено ја доставил Основната листа за проверка, дали е регистриран во *Централниот регистар на контролори и на збирки на лични податоци*⁴⁹ и слично). Инспекторот се подготвува и за содржинскиот дел од надзорот кој треба да го спроведе преку проучување на секторската легислатива во рамки на која контролорот работи, а се запознава и со профилот на контролорот на лични податоци. Профилот се формира преку истражување на информации за контролорот низ „Мрежата (WWW)“ и комуникација со Централниот регистар на РМ во врска со Регистарот на трговски друштва и други правни лица. Во одредени ситуации забележано е дека постои застој во комуникацијата со Централниот регистар поради кои не се добиваат навремено или воопшто не се добиваат податоци. Централниот регистар има обврска,⁵⁰ на Дирекцијата како институција која се финансира од Буџетот на државата и од други извори,⁵¹ да ѝ овозможи користење на податоците од регистарот без надомест. Доколку застојот е поради разлики во толкувањето на одредбата од чл.18-а од Законот за централен регистар во смисла дали Дирекцијата спаѓа во групата повластени институции или не, потребно е без одлагање да се покрене иницијатива за дополна на цитираната одредба. На овој начин на

⁴⁸ <http://dzlp.mk/mk/inspekcija>.

⁴⁹ Овој Централен регистар е база на податоци која ја води Дирекцијата. Таа се разликува од истоимена институција насловена како Централен регистар на РМ во кој се водат Регистарот на трговски друштва и други правни лица, Заложен регистар, Регистар на годишни сметки, Регистар за лизинг и други регистри.

⁵⁰ Според чл.18а од Законот за централен регистар (Сл.в. на РМ 50/2001, 49/2003, 109/2005, 88/2008 и 35/2011)

⁵¹ Чл.48 од Законот за заштита на лични податоци („Службен весник на Република Македонија“ бр. 7/05, 103/08, 124/10, 135/11)

Дирекцијата, (инспекторите), ќе им биде овозможен пристап до податоците од Регистарот во реално време (и on-line) со цел да се обезбеди висок степен на релевантност на податоците за правните лица кои се контролираат, како и рационалност и ефикасност во спроведување на надзорните активности.

Откако ќе се дефинираат деталите на посетата за надзор со овластените лица кај контролорот се спроведува посетата на лице место. За време на посетата инспекторот ги интервјуира релевантните вработени/овластени лица/офицер за заштита на лични податоци при што релевантноста на соговорникот зависи од видот на збирки на лични податоци кои контролорот ги гради. Надзорот кој може да се спроведе еднократно или пак може да се одвива и во текот на неколку дена односно во неколку наврати што пак зависи од обемот на збирките односно податоците кои контролорот ги собира. За време на надзорот инспекторот прави увид во документациите, начинот и процедурите за обработка на личните податоци, а прибира и докази со кои ги поткрепува наодите за неправилности во обработка и чување на лични податоци кај соодветниот контролор. Како доказ може да послужи документација (копии од актите со кои се уредува чувањето и обработката на лични податоци, договори, изјави, овластувања, фотодокументација која се креира на лице место, и други средства кои може да послужат како доказ. Наодот од надзорот се евидентира во Записник за спроведениот надзор кој во пишана форма се изготвува во рок од 30 дена од денот на завршување на надзорот (читај: последна достава на последен доказ кој контролорот го обезбедил за целите на контролата). Се чини дека во делот на рокови за достава на доказите од страна на контролорите да постои можност за голема флексибилност. Пожелно е во контекст на областа *Cloud computing* да се воведат поголема ажурност и да се воведат кратки рокови за достава на докази⁵². Постапката на надзор ќе заврши со подготовка на Записник за спроведениот надзор и со одлука на инспекторот. Согласно таа одлука инспекторот може да го затвори случајот, да донесе решение во врска со надзорот со кое ќе го задолжи контролорот да ги отстрани неправилностите⁵³, и во случај на повреди на Законот за заштита на лични податоци да преземе натамошни

⁵² Да се разгледа можноста за ревизија на регулативата во овој правец.

⁵³ За контролорот е обезбедена судска заштита преку можноста да поднесе тужба пред Управен суд против Решението на инспекторот.

мерки против контролорот и тоа покренување на прекршочна постапка пред Комисијата за прекршоци односно преку покренување на соодветна постапка пред друг надлежен орган (на пример: да поднесе Кривична пријава до јавно обвинителство заради сознанија/сомневања за сторено кривично дело).

Досега нема пракса при вршење на инспекцискиот надзор контролор да одбие да даде информации или да предаде документација која му се бара на увид. Но, инспекторот во случај да се сретне со таква ситуација овластен е да констатира дека контролорот нема информации/документација кои се бараат, а дополнително може да поведе прекршочна постапка поради оневозможување на инспектор да ја извршува својата работа.

Надзорот може да го спроведе еден инспектор, но контролата може да ја извршат и повеќе инспектори одеднаш како тим. Во тој случај еден од инспекторите на кој му е доделен предметот е носител и тој го води целиот предмет од почеток до крај. Носителот ја потпишува и документацијата која го следи предметот. Често кога има потреба во тимот учествува и инспектор со ИТ профил. Оваа пракса од гледна точка на темата која се анализира е позитивна пракса.

Во врска со *Cloud computing* спроведени се во текот на 2013 година 2 надзора каде е вклучено користење на услуги во „облак“. Во едниот случај контролорот е корисник на услуги во „облак“ додека во другиот случај станува збор за провајдер на услуга во „облак“. И во двата случаја се врши пренос на лични податоци надвор од државата.

Дирекцијата е персонално подготвена да врши надзор во врска со *Cloud computing*. Она што е потребно да се унапреди е начинот на кој се стекнуваат сознанија за тоа дали одреден контролор користи *Cloud computing*. Исто така имајќи ја предвид комплексноста на материјата континуирано следење на развојот во областа и едукација на инспекторите е важен елемент, иако во текот на јули 2011 година, инспекторите се сертифицирани со ИСО 27001. Со здобивањето со овој сертификат, инспекторите имаат зголемен капацитет за вршење на надзори во сложена ИТ инфраструктура на контролорите и обработувачите во различни сфери.

Вонредниот надзор се врши врз основа на иницијатива поднесена од орган на државна власт, правно или физичко лице, односно поднесено барање, како и во случај на сомневање на инспекторот за повреди на одредбите на Законот. За разлика од редовните контроли, посетите кои имаат карактер на вонреден надзор не се дел од плановите за работа на Дирекцијата, тоа се ad hoc посети кои може да бидат најавени, но и не мора. Може да се однесуваат на контрола на целата проблематика на заштита на лични податоци кај контролорот каде се спроведува надзорот, но логиката зад овој вид надзор е контрола поради конкретниот случај кој е пријавен или идентификуван од Дирекцијата но не трпи одлагање за да биде вклучен во планската документација.

Контролниот надзор е надзор за проверка на однесувањето на контролорот по констатирање на неправилности во смисла дали постапил по задолженијата за отстранување на утврдените неправилности, односно дали преземал соодветни мерки за намалување на ризиците за да се спречат идни злоупотреби на личните податоци чиј контролор е. За оваа посета на контролорот уште при констатирање на неправилностите му се дава рок во кој треба да постапи по забелешките и да ја поправи состојбата. Надзорот може да се најави, но по правило тоа не е потребно. Периодот во кој инспекторот постапува е 15 дена кои почнуваат да течат од последниот ден на рокот кој му би даден на контролорот да ги исполни задолженијата. За оваа посета се составува уште еден записник во кој се констатира нивото до кое постапил контролорот. Ако делумно или целосно не постапил по задолжувањата, инспекторот има право да поведе прекршочна постапка.

Во текот на последните три години и кај инспекцискиот надзор се забележува пораст на бројот на предмети, што е исто така резултат на интензивната активност на Дирекцијата. Подолу е прикажан трендот низ бројки.

Инспекциски надзор 2011 – 2013 според Годишните Извештаи за работа на Дирекцијата						
Година	Редовен надзор	Вонреден надзор	Контролен надзор	Пренесени предмети од претходната година	<i>Cloud computing</i>	Вкупно без пренесени предмети
2011	107	32	7	18	-	146

2012	273	95	-	28	-	368
2013					2	

Советување и едукација

Дирекцијата дејствува советодавно и во врска со областа *Cloud computing* како кон субјектите кои ги инспектира, така и кон пошироката јавност.

Дополнително, инспекторите во текот на надзорот имаат право, а субјектите кои направиле прекршоци откако ќе бидат констатирани на записник, а пред да им биде изречена казна да проследат едукација во врска со заштитата на лични податоци и особено во врска со повредите кои ги направиле.

Инспекторите од 2011 наваму со измените во Правилникот за инспекциски надзор имаат можност на контролорите кај кои се констатирани недостатоци и сториле прекршоци да се спроведе законска обврска за нивна едукација уште за време на надзорот што е позитивен чекор за ефикасна постапка. Ваквиот пристап во дигитална средина е особено значаен – брзо и ефикасно постапување.

14. ПРЕПОРАКИ И ЗАКЛУЧОЦИ

- 1) Да се продолжи со промоција на улогата и позицијата на Дирекцијата за заштита на лични податоци во генерална смисла за да се запознаат граѓаните колку е можно повеќе со нејзиното постоење и надлежности, зголемување на свесност на граѓаните.
- 2) Да се преземат активности за проценка на свесноста на јавноста и истовремено зголемување на свесноста поврзана со заштитата на лични податоци и интернет;
- 3) Во контекст на планирање и следење на областа да се воспостави соработка со Државниот завод за статистика и во тој контекст да се воведат во прашалниците за анализа на Информатичко општество прашања со кои ќе се следи состојбата со *Cloud computing* и социјални мрежи за деловните субјекти и јавната управа, како и за физичките лица

- 4) Да се унапреди соработката на Дирекцијата со други институции кои имаат надлежност во област на електронски комуникации како што е Агенцијата за Електронски комуникации, Министерството за информатичко општество и администрација, Министерство за транспорт и врски, Централен регистар итн.
- 5) Да се унапреди соработката со организации од бизнис секторот како што се на пример социјални мрежи или провајдери на *Cloud computing* преку потпишување на Декларации или Меморандуми за соработка;
- 6) Да се унапреди соработката со организациите од образованието на сите нивоа (Министерство, локална самоуправа, училишта) заради унапредување на свесноста на професорите, наставниците, младите и децата за правото на приватност и заштита особено на социјалните мрежи. Дополнително, оваа препорака да се надгради на веќе постоечки Проект кој се занимава со приватноста во образованието финансиран од ЕУ;
- 7) Со оглед на фактот дека организациски Дирекцијата засега ги задоволува потребите, заради понатамошно зголемување на ефикасноста во работата со сегашната поставеност на Дирекцијата се препорачува да се унапредат алатките со кои Дирекцијата работи. Да се спроведе ревизија на Листата за проверка која се испраќа до контролорите пред спроведување на редовен надзор во смисла да се воведат прашање(а) за употреба на *Cloud computing* односно социјални мрежи за контролорите на лични податоци. На овој начин ќе се овозможат сознанија за користење на овие сервиси од страна на контролорите и пред да започне инспекцискиот надзор. Ова особено е важно во контекст на *Cloud computing* бидејќи користењето на овие услуги не секогаш е лесно достапна информација до која може да се дојде од јавни извори;
- 8) Во врска со организациските капацитети на Дирекцијата за постапување со предмети поврзани со социјалните мрежи потребно е да се зголеми бројот на лицата кои ќе работат во оваа област со реалокација на одговорности ако не со ангажирање на нови лица. Ова особено важи во контекст на идните активности кои треба да се преземат во рамки на овој Проект како што е „Тимот за поддршка“ и Веб платформата за помош на лица кои сметаат дека им е

повредено правото на приватност односно злоупотребени им се лични податоци на социјалните мрежи.

- 9) Иако контролата во врска со *Cloud computing* која до сега е вршена кај контролори кои ја користат ваквата услуга е солидна, сепак потребно е да се посвети повеќе внимание на правните аспекти на заштитата (во смисла на проценка на содржината на одредбите кои се користат/недостасуваат во меѓусебната соработка на партнерите на контролорот и контролорот сам по себе).
- 10) Да се ревидира легислативата во смисла да се третира *Cloud computing* како трансфер на податоци во странство, па да се задолжат контролорите да побараат одобрение за трансфер за користење на *Cloud computing* сервиси;. Дополнително да се воведо обврска во секој случај контролорот да биде обврзан да поднесе Известување до Дирекцијата пред да започне со користење на вакви сервиси;
- 11) Да се воведо обврска до контролорот кој има намера да користи *Cloud computing* услуги кон известувањето да достави стандардна Листа за проверка на провајдерот и усогласеноста на услугата со регулативата за заштита на лични податоци;
- 12) Да се направи широка анкета помеѓу граѓаните за да се констатира состојбата со нивниот став кон начинот на кој пристапуваат за заштита на сопствената приватност, за да релевантно се насочат активностите на Дирекцијата во иднина.

Анекс 1 - Органограм на ДЗЛП

