04

E-Newsletter

Directorate for Personal Data Protection

December
2013

In this issue:

Dear readers,

We have the honor and pleasure to introduce you with the fourth edition of the E-Newsletter of the Directorate for Personal Data Protection of the Republic of Macedonia.

This time we shall inform you about our activities and initiatives, trying to continuously promote the right to personal data protection and the right to privacy of the citizens.

In relation to this goal is the initiative "Ambassador for Personal Data Protection". We are deeply convinced that every society should create an environment where laws, services and behaviors in practice reduce the risk from abuse of personal data for every person individually, whether he/she is a public figure or not. And yes, the title "an Ambassador" does not in itself mean a privilege for something, but also an effort, personal and professional, to clearly and firmly establish a culture of respecting the privacy of others.

One of the priorities of the Directorate is further strengthening of regional cooperation.

We briefly mention the issue of video surveillance on the workplace/ employees, as well as treating issues from hotels/travel agencies area regarding the protection of personal data, as the challenges in the Schengen zone too..

Dear readers,

With the aim of continuously presenting knowledge to you for various topics related to your right to personal data protection and right to privacy, we are deeply convinced that you will find interesting information in this edition of the E-Newsletter as well.

In light of the upcoming holidays, I wish you a Merry Christmas and a Happy New Year!

Director,

Dimitar Gjeorgjievski

"I own my privacy"

DPDP

Bilateral Meeting - Kosovo

On October 25, 2013 a delegation from the National Agency for Personal Data Protection of Kosovo visited the Directorate for Personal Data Protection.

The purpose of the meeting was further strengthening of the cooperation and sharing experiences from the development of both authorities. The colleagues from the Republic of Kosovo showed special interest for the implemented Software for Inspections supervision (SIN) in the Directorate for Personal Data Protection, as well as the possibilities to expand and intensify the cooperation.

"Ambassador for Personal Data Protection"

On 10 November was the new initiative "Ambassador for Personal Data Protection", whose holder is Mr. Arben Shaqiri, a famous Macedonian rock singer was promoted. The promotion was followed by the signing of a Memorandum of Mutual Cooperation.

This is only one piece of the planned activities of the Directorate to establish communication with specific target groups, especially young people.

In order to raise the public awareness, especially in the category—young people, we are confident that the nomination of public persons as "Ambassadors for personal data protection", whose opinion, behavior and actions, both personally and professionally, are set as an example, especially among the young population, will certainly and directly impact the creation of a culture for protecting the citizens' privacy, as well as greater awareness regarding personal data protection in Macedonia.

According to the data of the Directorate for Personal Data Protection, during this year (from 01.01.2013 - until December 1, 2013) a total of 219 complaints for abuse of personal data on the social networks have been received, 203 of which apply only to the abuse of the social networking site Facebook, and 16 of them apply to the other social networks.

The numbers that the Directorate has indicate the need to act in education area, especially considering the fact that the young people are the most common users of the internet and social networks, this only confirms the fact that every activity in terms of prevention is going to have long –term results.

FB Directorate for Personal Data Protection www.dzlp.mk

UNDER THE WATCHFUL EYE OF THE BOSS!

By: Elena Stojanovska, M.A.

May the employees in factories, confections, manufacturing plants be monitored by the employer through a video surveillance system and may hidden video cameras be set up for this purpose?

Employers and employees are often subject to discussions about the implementation of the laws for personal data protection. Regardless of whether the privacy of the employees is protected by law, respecting it is considered an added value in the working culture of a company. Employees expect privacy at the workplace, although they are in the company's premises and use the company's equipment.

Very often, in official premises, video surveillance is installed for which there are many specific provisions in the Law on Personal data Protection. Namely, the employer can conduct video surveillance in official premises if that is necessary for protecting the lives and health of the employees because of the nature of the job or securing control over the entry and exit from the official premises.

In the indicated case of video surveillance of the employees in factories, confections, manufacturing plants, the system can be set up, but only for protecting the life and health of the employees due to the nature of the job (for example, if working on specific machines could endanger the physical health of the employee). While setting up video surveillance in this places, it is mandatory to pay attention to the angles and the resolution of the camera.

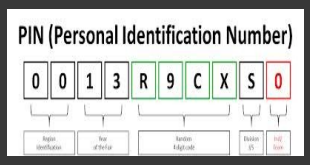
The employers must notify the employees that video surveillance is conducted in the official premises, installing hidden video cameras by the employer represents a clear violation of the provisions from the Law on Personal Data Protection. If the employer wants to install visible cameras for the listed purposes, he/she shall be obliged to regulate the manner of conducting video surveillance with a special act and to notify the employees about the cameras, i.e. the video surveillance. In the Law on Personal Data Protection, the places where it is prohibited to conduct video surveillance are specified. Those are lockers, changing rooms, toilets, elevators and other similar rooms. The increased interest about the implementation of the principles for personal data protection, but also the increased number of complaints that the Directorate has received regarding the protection of privacy at the workplace, especially when using video surveillance were the stimulus for the Directorate and the Textile Trade Association—Textile Cluster to sign a Memorandum of Cooperation.

By the end of this year, various trainings for the members of the Cluster regarding the implementation of the provisions for personal data protection in performing their work are going to be conducted. By signing this Memorandum, the Directorate for Personal Data Protection and the Textile Trade Association—Textile Cluster have emphasized their commitment to upgrade the implementation of the provisions for personal data protection in this field in the Republic of Macedonia.

Initiative for an irregular inspection you can find it HERE

Request for confirming violation of the right of personal data protection

Download HERE



My Identification Number

By: Liljana Pecova-Ilieska, M.A.

According to Article 9 from the Law on Personal Data Protection, the identification number of the citizen can be processed only when:

- "after receiving previous explicit consent by the subject of personal data; to exercise rights and obligations of the subject of personal data or the controller determined by law and other cases determined by law. The controller shall control that the identification number of the citizen is not unnecessarily visible, printed or downloaded from a collection of personal data."

In the Republic of Macedonia there is a unique identification number for the citizen. Lately, there have been numerous debates about establishing another number to identify the citizen from the aspect of a tax number. But, on the question whether this is a positive practice regarding personal data protection, we consulted Rosana Lemut-Strle, L.L.M, deputy Commissioner for Information from the Republic of Slovenia, who said: „In the Republic of Slovenia, individuals have three personal identification numbers, which define us completely, namely the personal identification number, tax number and the health insurance number. The dilemma about whether it is better/safer to use only one identification number, which completely defines an individual or more for different fields – from the point of view of the safety of personal data – is still present in Slovenia.

The idea of using special identification numbers exclusively for individual fields – the field of taxes and the field of medical services in the public health system – has not been realized completely, but at least to a large extent. The tax authorities use only the tax number to communicate with the person liable for tax within their procedures and those providing medical services in the public health system use only the health insurance number to communicate with the insured person and the provider of the compulsory health insurance .

Such an arrangement makes it difficult to easily connect data on an individual's personal status (residence, marital status, number of children ...), his/her property and health status to all who are not familiar with all three of his/her identification numbers. Those who are familiar with them, because they keep them in their records in accordance with the law, can of course use them only for carrying out their legal jurisdictions. We could say that such a solution is more favorable to the protection of privacy and personal data. The competent authorities have data that they need while all others can access only to "parts" of an individual's identity. The Slovenian regulation seems difficult and hard to carry out, thus the ideas about cancelling the personal identification number reappear from time to time.

The personal identification number is generally "the least desired" identification number. It gives away a lot of our personal data in its structure (the date of birth, gender, and still following the historical pattern from the ex-Yugoslavia the nationality as well ...), while the tax number and the health insurance number, are actually only numbers. Regardless of this, there are not any serious reservations regarding the valid legislation which would start a legislative initiative.

Slovenia – as a country with a bit more than two million inhabitants – has to be even more attentive to its privacy and protection of personal data. The more inhabitants there are the better they can "hide" in the crowd as individuals and the less broad circles of acquaintances which can include whole settlements they have etc. It is easier to protect one's privacy in bigger communities than in smaller. Therefore it is important to ensure that individuals in smaller communities have an efficient opportunity to keep for themselves the data that they do not want to share – even before the state authorities, when these data aren't necessary for carrying out their jurisdictions.

Hello, reception desk?

By: Elena Stojanovska, M.A.

Which personal data hotels may collect about their guests and may they keep the passports of foreign guests and or identification cards of domestic guests?

Different work practices of the hotels often cause dilemmas at guests about the personal data they should give when registering in a hotel, whether the receptionists may keep the ID card and/or the passport?!

The obligation of the guests to give personal data when entering in a hotel is clear, but the amount of personal data needed and necessary for the hotel is the cause of confusion.

According to our Law on catering activities, hotels have a Book of domestic guests and a Book of foreign guests that according to the Law on personal data protection are collections of personal data.

The Book of domestic guests includes the data about ordinal number, name and surname, date and place of birth, permanent address, ID card number, room number, day of arrival, day of departure and notes.

The book of foreign guests contains data about ordinal number, name and surname, date of birth, place and country of birth, citizenship, type and number of passport, type and number of residence permit, date of expiry of the residence permit, address and apartment, apartment owner, address of the owner, date of registry, date of entry in the Republic of Macedonia and border crossing.

This books have to be kept locked and access to them to be allowed to the receptionist that is working at the moment.

Following this provision and principles of personal data protection, keeping the ID card of domestic guests or the passport of foreign guests is not according to law i.e. this documents may be asked for the purpose of entering the required data in the books, but they can not be kept during the stay of the guest in the hotel.

Hotels have the obligation to fill a form according to the Law on Registration of the Residence of the Citizen and its submission to the Ministry of Internal Affairs, with which the data about the name and surname, day, month, year, place, municipality of birth, place of permanent residence, ID card number, date and time of arrival, notes, signature of the user of services and signature of the landlord. Hotels as controllers of collections of personal data have the obligation to adopt acts for technical and organizational measures fore securing secrecy and protection of personal data as well as a rulebook about the manner of conducting video surveillance as a very important part of their work.

Video surveillance in hotels can be used for security purposes and protection of the ownership and it can be set in the hotel's official premises as well as the space around the hotel, but it can not violate the privacy of the guests. Access to the video surveillance room should be regulated and limited to authorized persons that have signed a non-disclosure statement through the video surveillance system.

With the purpose of better understanding of the hotels and travel agencies about the obligations that arise for them from the Law on Personal Data protection, the Directorate for Personal Data Protection and the Trade Association for Tourism of the Republic of Macedonia have signed a Memorandum of Cooperation according to which trainings for secrecy and protection of the processing of personal data shall be organized.

The purpose of these trainings is to intensify the activities regarding the Law on Personal Data Protection, the implementation of the documents for technical and organizational measures for securing secrecy and protection of the processing of personal data and the implementation of the provisions that refer to the processing.

TRAINING in the DPDP

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

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

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

Information on Training Program for provision of secrecy and protection of the processing of personal data and **Request** for applications for training can be found at the following **link**

Directorate for Personal data Protection

Status: independent public authority with status as legal entity

Management: Director and Deputy Director

Responsibility: Before Parliament by submitting an Annual report on the work of the Directorate

Financing: Budget of the Republic of Macedonia and partly own income

Legislation: Directive 95/46/EC on the protection of personal data and the free movement of such data

Convention no.108 on the protection of individuals regarding the automatic processing of personal data by the Council of Europe since 1981

Additional Protocol to the Convention regarding supervisory authorities and cross border transfer of data

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

Introducing the EUROJUST values

By: Marjana Popovska, L.L.M

EUROJUST is a body of the European Union established in 2002 as legal entity and headquarters in the Hague, Kingdom of the Netherlands. Basic mission of EUROJUST is to strengthen the effectiveness of the Member States institutions competent to investigate and prosecute serious forms of transnational and organized crime. EUROJUST has a unique role in the legal field of the European Union and its main purpose is to improve the development of Pan– European cooperation on criminal cases.

During 2008, the Republic of Macedonia began the negotiations with EUROJUST with the purpose of signing a Cooperation Agreement. At the same time, during the negotiations it was determined that one of the main assumptions for signing this agreement is to establish an adequate system of personal data protection in the Republic of Macedonia with the authorities with special authorization according to law, that resulted in adopting the Law on Modification and Amendment of the Law on Personal Data Protection and deleting the part contained in the Law on the Ratification of the Convention for protection of physical entities regarding the automatic processing of personal data, which refers to the fact that this Convention shall not be applied when conducting criminal proceedings. After the completion of this processes on November 28, 2008 the Cooperation Agreement between the Republic the Macedonia and EUROJUST was signed and published in the "Official Gazette of the Republic of Macedonia" No 51 from 2009.

According to the provisions of Article 17 from the Law on the Ratification of the Cooperation Agreement between the Republic of Macedonia and EUROJUST, it has been established that the national authority for personal data protection (in this case: the Directorate for Personal Data Protection) in the Republic of Macedonia submits a Report on an annual basis to EUROJUST about the conditions in the judiciary field (public prosecutors) regarding the implementation of the provisions for personal data protection. The purpose of this Report is to present the actual condition in the public prosecution offices in the Republic of Macedonia regarding the implementation of the provisions for protection of the processing of personal data.

Starting from the need to find the adequate balance between legitimate processing of personal data and undertaking measures and activities in the fight against terrorism and organized crime and protection of the privacy of individuals, regulating the protection of personal data is of great importance to realize the cooperation with EUROJUST. At the same time, to establish full operative cooperation with EUROJUST, it is necessary to establish an adequate system for protection of personal data in the judiciary field.

With the purpose of preparing this Annual Report regarding the implementation of the provisions for personal data protection by the public prosecution offices and according to the Annual Program of the Directorate for Personal Data Protection and Monthly Plans for Conducting Inspection in 2013 (March, April, May, June), 30 regular inspections were conducted over the legality of the activities undertaken when processing personal data and its protection in the public prosecution offices that included the Public prosecution of the Republic of Macedonia, the Council of Public Prosecutors of the Republic of Macedonia, the Academy for Judges and Public Prosecutors, Senior Public Prosecutors (4 total), Basic Public Prosecutors (22 total) and Basic Public Prosecution for prosecuting organized crime and corruption.

Subject of analysis during the inspections were the collections of personal data that the public prosecutors keep while conducting their competences determined with the provisions of public prosecution (personal data about suspects/accused/sentenced persons, witnesses, victims, authorized persons) and the collection for video surveillance.

Preparing this Report about the implementation of the provisions for protection of personal data and submission to EUROJUST is of crucial importance for our country in the process of accession to the European Union. This is especially important for the need to exchange personal data between EUROJUST and the public prosecutors can be conducted only if the basic rules of international data exchange are applied, the data delivered must be checked for accuracy and reliability, to be updated as well as there has to be a legal basis for its exchange.

The Directorate for Personal Data Protection actively participated in the adoption of the new Law on Criminal Proceedings, continuously mentioning the need for balance between public interest, especially the measures that have to be undertaken in the fight against crime and respecting the right to privacy by the authorities for conducting the law.

In that direction, the State Public Prosecutor of the Republic of Macedonia, Mr. Marko Zvrlevski said:

In the fight against crime and terrorism, we must not forget the basic human rights and freedoms, rather it is necessary to secure their protection. Following this, in Chapter XV from the new Law on Criminal Procedure that shall be applied from 01. 12. 2013, provisions about the protection of personal data during criminal proceedings that refer to the processing of personal data by the court, public prosecution and other authorities with special authorization.

In that direction, establishing the legal framework for the processing of personal data by the public prosecutors for the needs of criminal proceedings is especially important, because of which the public prosecutors have paid great attention with the purpose of harmonization with the European and world standards. To proceed according to the standards, we express readiness to accept the suggestions, recommendations and indications of the relevant and competent institutions, especially from the Directorate for Personal Data Protection."

http://eurojust.europa.eu/about/background/Pages/History.aspx

Schengen Border Code — A Challenge for the Protection of Personal Data

By: Snezana Trajanovska, L.L.M.

At a time when the movement of people and goods across borders is one of the basic tenets of modern living, arrangements of standards and uniform approach in performing border controls for EU for many years was a kind of challenge. Even in 2006 was for the first time enacted a comprehensive document that systematically establishes the rules for the free movement of people, in terms of the EU without internal borders - Schengen area, i.e. "Community Code on the rules governing the movement of persons across borders" (Schengen Border Code). The document is fully binding and directly applicable in all Member States of the EU, according to the Treaty establishing the European Community and since then until now, it has undergone several amendments.

Relatively limited information regarding the protection of human rights and freedoms, including the protection of personal data, inevitably open a new "front" for all entities participating in the implementation of the document, thoroughly to devote to the study the essence of the reference documents that the Code indicates in order to properly implement its provisions in practice. For example, while a document from 2006, item 20 of the Preamble states that: "This Regulation respects fundamental rights and observes the principles recognized, in particular the Charter of Fundamental Rights of the EU. It will be applied in accordance with the obligations of EU member states regarding international protection and non-return", with the amendments from June 2013 it was introduced a special Art. 3-a entitled "Fundamental Rights" , in which a lot is explained in more detail the scope of the obligations of the Member States. Given that one of the fundamental freedoms, noted in the Charter of Fundamental Rights of the EU, is the protection of personal data, with the Lisbon Treaty, it acquired legally binding force equal to that which the founding treaties have, then it is clearly to what level is elevated the importance of the application of this freedom.

Protection of foreigners and their data about a travel is foreseen through the possibility at the request of the person not to perform input of exit/entry seal in travel documents, if such entry "could cause serious difficulties for that person" (Article 10) but it is executed on a separate form/sheet.

The Authority collects statistics on such cases and submit them to the European Commission.

Article 5 provides for compulsory screening in SIS (Schengen Information system) as a step in deciding to join the Schengen area, thusly officers carrying out border checks must be thoroughly familiar with the rights of individuals controlling, especially when personal data are entered incorrectly, out of date termination of the "warning", cases of identity theft and so on. The person whose data are entered in SIS, has the right to request access and be assured that they are accurate and filed in accordance with the law, except when it comes to taking legal action over "warning" and protect the rights and freedoms of others. The obligation of each state to set up a special body responsible for the introduction and use of data in SIS (i.e. SIRENE Bureau) further shows how much importance is given to managing this huge database.

Registration Information by border crossings is regulated by Annex 2 of the Code providing that all official information and other important data especially recorded manually or electronically, and apply multiple categories, such as names of officials responsible for border checks and their data about holding stamps, arrests and complaints, people who have been denied entry, complaints from persons who undergo checks, etc. In order to provide the necessary preconditions for the proper implementation of established standards, the Code imposes a duty on Member States to train staff on the rules of border control and fundamental rights. In order to facilitate the daily operations of border officials, a separate Manual is prepared with examples of practice and advice for proper treatment, that regularly is updated in compliance with the Code.

Finally, in one article of Annex 6, the Code specifically addresses the protection of personal data drawing generally a limit of the ability of employees to access IT systems for processing of personal data (Article 7) in which "it is allowed to Member States to establish technical and organizational security measures, established by Union legislation to protect personal data against accidental or unlawful destruction or sudden loss, unauthorized disclosure or access, including access to the bodies of third countries" (countries that are not EU members) .

Conclusions:

1. The Code in case of personal data protection gives the general framework through the obligation to apply the relevant provisions prom the Charter of Fundamental Rights of the European Union (Annex B).

2. Every Member State (as well the countries that are in the process of accessing the European Union should work on strengthening their administrative and technical resources using the best practices and exchange of, as well as relevant manuals for detailed elaboration of “sensitive issues”.

3. To reach the necessary standards when conducting border control, necessary trainings, professional upgrade, experience and total commitment of the competent border services for every individual case.

4. Everything mentioned above is a prerequisite (and maybe it is not an exaggeration to say *sine-qua-non*) for the successful implementation of Schengen Border Code, especially regarding the use of enormous bases of data, where personal data protection is subject to rigorous standards.

The legislative base for the functioning of SIS, вis found in two acts:

Regulation No.1987/2006 of the European Parliament and the Council from 20.12.2006 for establishing the work and use of the Schengen Information System’s second generation (SIS 2), and

Decision 2007/533/PVR of the Council from 12.06.2007 for establishing, working and the use of the second generation of the Schengen Information System (SIS 2).

Could you please give me an information on the following: I have a final and binding judgment that the debtor should return me certain amount of money. At the same time, the debtor has alienated the apartment to a third party with a Notary act. Is the enforcement agents and/or I may ask from the company he works in to submit data for the loan that the debtor pays, the name of the bank has entered into an agreement, the installment amounts, if the notary is obliged to issue a copy of the request of the executor?

Dear Madam/Sir,

According to Art . 34 of the Law on protection of personal data the controller will give personal data to the user, based on written request from the user, if they are required to perform work within the legally established responsibilities of the user. The written request must include: the reasons, the legal basis for the use of personal data and the category of personal data are required.

In this particular case, only an authorized person, the executor, according to Law on enforcement has the right to collect data on the assets of the debtor for the purpose of performance execution, to conduct an inventory, assessment, seizure and sale of movable property, rights and property, receives funds and submit a request for data having the accounts relating to the subject matter of execution.

I work in the Center for Social affair in the area of changing personal name, regarding when the party seeks to change personal name or surname. Previously we requested a copy of identity card, birth certificate and if it comes to divorce and a copy of the judgment of the Court. Because it is a change of personal name/surname and identity card was our basic document for performing change of data, please give me an explanation whether or not we may require or not a photocopy of the ID card.

Dear Madam/Sir,

Please note that in accordance with Article 6 of the "Law on protection of personal data", personal data processing may be performed after prior consent by the data subject to fulfillment of legal obligations and legitimate interests of the controller for execution of works of public interest in the official authorization of the controller .

The identity card as an identification document can serve only for review and to determine the identity of the person. Copy, scan or retention of an ID card is considered unlawful processing which process personal data with volume greater than necessary to fulfill the purpose for which this document is requested for.

It follows that there is no legal basis for the processing of photocopies of ID and if there are in your possession it should be destroyed by a Commission in accordance with Art. 20, paragraph 4 of the Regulation on technical and organizational measures to ensure confidentiality and protection of personal data (" Official Gazette" , br.38/09 158 /10) .

You can send your questions/dilemmas to:

info@dzlp.mk

Request for confirming violation of the right of personal data protection

info@dzlp.mk

Download HERE

Dearth of Anti-Peeping Laws Will Cost Sweden

(CN) - European countries violate privacy rights if they lack laws on the books that prohibit secret videotaping or picture taking, the European Court of Human Rights ruled.

The ruling stems from a case in Sweden where a man secretly videotaped his stepdaughter while she took a shower. Although a court originally convicted the man of sexual molestation and ordered him to pay restitution, a Swedish appeals court reversed the conviction after finding that - since the man never touched the girl - the surreptitious videotaping without the girl's consent in and of itself was not a crime. The appellate court admitted, however, that the outcome would have been substantially different for the man had prosecutors charged him with child pornography.

Years later, the girl took her case to the European Court of Human Rights. She said that despite years of wrangling over laws that would have protected her legally, Swedish lawmakers had done nothing and the government violated her right to privacy by failing to provide her with adequate remedies against the stepfather. Despite the Swedish government's argument that the human rights court could not step in the middle of what was essentially a dispute between two people, the Strasbourg-based court agreed with the girl last week.

"Regarding the protection of the physical and psychological integrity of an individual from other persons, the court has previously held that the authorities' positive obligations may include a duty to maintain and apply in practice an adequate legal framework affording protection against acts of violence by private individuals," the court wrote.

"In respect of children, who are particularly vulnerable, the measures applied by the state to protect them against acts of violence should be effective and include reasonable steps to prevent ill -treatment of which the authorities had, or ought to have had, knowledge and effective deterrence against such serious breaches of personal integrity," the justices added. "Such measures must be aimed at ensuring respect for human dignity and protecting the best interests of the child." Link

Call for better privacy protection in the cloud

It might be easy to click "I agree" on the bottom of endless software end user licence agreements (EULAs) without a second thought, but when it comes to putting one's data on the cloud the one-size-fits-all approach needs to be overhauled, according to University of Illinois IP and technology law professor Jay P Kesan.

Professor Kesan says people need to be better informed about what happens to their data when they accept terms and conditions. He warns that as long as we find it perfectly acceptable to give personal information to online services, it allows their owners to snoop, aggregate and data mine our online habits as they see fit. Kesan and colleagues surveyed the EULAs of 19 major online services (including Amazon, Google, Microsoft, Dropbox, Facebook, Flickr, Cisco, Salesforce and VMWare) and found that providers were consistently more detailed when describing user's obligations to them than the other way around...It might be high time for more transparent cloud service agreements. The sector shows no signs of slowing down, and Google raised eyebrows when company lawyers told a US court that 'all users of email must necessarily expect ... emails will be subject to automated processing'. This week, it was revealed Australian jobseekers are having their medical examination results supplied to potential employers. Many already feel jittery about the cloud.

Some 33 per cent of respondents to a survey from social research company 1WorldOnline said security concerns keep them from using cloud storage, and as reported in August, the US cloud computing industry stands to lose $38.7b after revelations about the extent of private data snooping by the NSA. Kesan says cloud EULAs are deliberately fuzzy and one sided, giving the providers legal wiggle room around whatever privacy laws exist. "There's virtually no way for a consumer to know what the 'industry standard' practices are for protecting personal information, for example," he says. "Vague assurances don't provide an effective baseline and can undermine efforts to enforce a company's privacy policy against it." Link

Contact:

Directorate for Personal Data Protection

Blvd. Goce Delcev 18

1000 Skopje, Macedonia

tel: ++389 (0)2 3230 635

fax: ++389 (0)2 3230 635

E-mail:

info@dzlp.mk

info@privacy.mk

web:

www.dzlp.mk