Directorate-General for Justice, Freedom and Security
Unit D5 – Data protection
B - 1049 Brussels

Opinion of the Association for Fair Data Processing

This document was elaborated in response to the call for public consultation on the legal framework for the fundamental right to protection of personal data

Budapest
2009

Introduction

The Association for Fair Data Processing (A Tisztességes Adatkezelésért Egyesület in Hungarian) was founded on 6th November 2009 in Budapest, Hungary. This informal association consists of independent scholars, legal and information technology experts. Its aim is to discuss newly emerging problems with respect to personal data protection and freedom of information.

1. Definitions

The Association for Fair Data Processing would like to suggest clarifying certain definitions of the European Data Protection Directive.

1.1. What is *personal* data?

In Article 2 of the Directive 95/46/EC (DPD) a short sentence defines the concept of personal data: "*(a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject');*". This formula might be replaced by a clearer one that mentions also that any conclusion that can be drawn from existing data is also personal data. The definition shall refer to some special kind of data, like biological samples (tissue, blood, cell culture), biometric identifiers (fingerprints, palm prints, retina images, facial images, etc.), live camera recordings, still camera images, voice prints, national unique identifiers and any personal attributes connected to these identifiers.

1.2. Special categories of personal data

It is advised, that those personal data that have been collected in the interest of national security would be included in *special categories of personal data*. Among the reasons for this we can mention, that such data most probably contain information about the societal connections, belief, health, criminal history or sexual connections of the data subject, not to mention the method and nature of the collection of the data. As being special (sensitive) personal data, this shall affect the future of the collected data.

1.3. Data concerning to deceased persons

Strongly connected to the previous question is when personal data does cease being *personal*? The legal tradition across Europe considers that only living human beings (natural persons) may have *personal* rights. It follows from that the right for protecting personal data – which is a personal right – can only belong to a living human. That means, when people die, they lost their rights to protect data that are related to them. We don't think that this is a *fair* solution.

What does *respect family life* mean in the Article 8 of ECHR?

Let us consider the Article 8 of the European Convention on Human Right (ETS-005, Rome Treaty, 1950). It mentions that people have right to protect their *family life*. This projects forward that many of the personal information collected by the governments really are not *personal* but *family* related information. When a piece of information is given by an identified human, this information strongly connected to a well identified member of the society, but the data in fact **relates to** his/her family. If we think of this fact, we will see that all health information, banking account information, investment information, living conditions, spending customs, travel and leisure customs, faith, world view are family related information. Therefore when someone dies, we must not say, that the information left behind

is not related to anyone living human. Instead, the information from that time, still relates to the spouse (widow), children, grandchildren of the family.

The governments do not take this into consideration. The Hungarian Parliament entered the new Human Genetic Act (Act 21 of 2008) into force that requires written consent before giving genetic sample and a separate consent before the data/sample being stored. At the same time the Parliament enabled deliberately use deceased bodies to obtain tissue samples from them for research purposes. Other (non-genetic) kinds of medical data of the deceased can freely be used for medical research without informing the relatives, or asking permission to use the data. Personal data of other non-genetic type are deliberately used as information mine (resource) at the next second after the death of the data subject.

Therefore we suggest that the commission would rule out, that if the personal data relates to some members of the data subject's family, then it remains *personal* data after the data subject's death. Moreover, the heirs (family members) have right to ask the data to be deleted if there are no legal reasons to retain them for a certain period (in this latter case the data shell be deleted right then as the retention period expires). When the data processor want to process data and normally it requires consent from the data subjects, but the data subject is already dead, in that case the consent shall be given by the widow or children of the deceased. When no living heirs can be found, then the Paragraph 2 of the Article 11 (*Paragraph 1 shall not apply where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law. In these cases Member States shall provide appropriate safeguards*) can be applied.

In some rare cases, when the law allows, the data subject's family may require a copy of the stored data. The European Court of Human Rights in Strasbourg decided that children may obtain personal health (genetic) data of their parents if getting to know this information is in their life interests. In other case family members are not entitled to get a copy of personal data of a deceased ancestor. One can find similar rulings in the French Data Protection Act.

1.4. What is consent?

Out association would advise, that the Directive shall clearly describe the meaning and properties of the consent. In the Article 2 of the Directive (*(h) 'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.*) we found that this definition says nothing about the revocability of the consent. This should be included in the definition.

In some cases consent is implied, especially in healthcare. In that case the Directive shall rule out, that a written version of the consent (that is implied) shall exist and this document is of public interest. Data processors must put out on the internet so as prospecting data subjects can get to know what is implied. We propose also to clarify further the content of the expression "freely" given indication.

1.5. What is *independent manner*?

Data processors may nominate data protection officials who act in independent manner. A clearer definition is needed on what does independent mean. Can an employee be independent from the point of view of the 95/46/EC Directive, what shall be the criteria of the independence?

2. Data processing for national security

According to Article 3 (2) of the DPD the directive does not apply to the activities carried out by – among others – secret services, thus Article 13 gives them further exemptions. We understand that the detailed regulation of the processing of personal data for national security purposes is the duty of the national legislative bodies. Even then it should be considered, that some broad concept on the protection of the individuals regarding their absolutely protected core area of their private life. Therefore we see to be necessary to have some general guaranties for this kind of the processing of personal data in the general EU data protection act (e.g. defining the data storing and using for security purposes as sensitive data, or making specific provisions for informing the data subject about this kind of procession etc.) In that respect we refer to the milestone judgment of the German Constitutional Court / BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. (1 - 333).

3. Data processing for avoiding crimes

We would like to make a reference to the 21.Declaration of the TFEU which sais that "The Conference acknowledges that specific rules on the protection of personal data and the free movement of such data in the fields of judicial cooperation in criminal matters and police cooperation based on Article 16 of the Treaty on the Functioning of the European Union may prove necessary because of the specific nature of these fields." We are sure that the general principles of the protection of personal data have to be applied in this field also for ensuring the rights every EU citizens; therefore it is necessary to extend the scope of the new legislation to the fields of police and judicial cooperation in criminal matters also. Furthermore we think that it would be necessary to provide the suitable guaranties of using new technologies for data processing for these purposes (e.g. processing the DNA and fingerprint for law enforcement purposes or using video surveillance equipments for the purpose of crime prevention e.g.)

4. Processing personal health data

The recent technical development in the area of health data processing requires urgent data protection interventions. We would like to refer to 2009/C 128/03 document of the European Data Protection Supervisor (EDPS). From this document it can be seen, that even the definition of the *personal health data* is not clear. Generally, the governments would like to treat some administration data as non sensitive data (referrals, admissions data) – although it has strong connection with the health status of the data subjects.

From the data protection view the national health insurance systems pose big threat to personal dignity, because these systems intends to store health related personal data of all insured citizens including newborns and pensioners as well. The insurance systems collects more and more detailed personal data and keep them lifelong, even after death. Health insurance systems usually collect diagnose (ICD-10) codes of any medical events beginning with cough, diarrhea to menstrual cramp. Using this data, a detailed medical history of any identified insured people can be obtained and analyzed. The second threat to the personal dignity is the database of a large medical complex (network of hospitals, ambulances, clinics), where tremendous amount of medical information is stored about people living nearby.

According to the 95/46/EC Directive, Article 8 (4) and preamble 34, governments make health insurance systems working by the force of the law, because of substantial public interests. Can we say that the amount of the collected data and the retention time are proportional to the goal of the processing? Absolutely, are not. Personal insurance data is kept for unimaginable long time with minimal protection, and deliberately used in state administration, health planning, national security inspections, medical research done by government bodies etc.

According to 95/46/EC Directive Article 8 (3) it is not clear, that the basis of the processing of personal medical data at health care providers is the written consent of the patients or it can be enforced by the law. Anyway, Hungary has a Health Data Protection Law that makes all medical data processing obligatory and disregards patient rights established in the 95/46/EC Directive, the ECHR, the Strasbourg Treaty and Ovideo Treaty. Even participation in medical database research is enforced by the law, neither preliminary information nor consent of the data subjects are not needed.

29. Working Group on Data Protection issued the Working Document 131 on EHR (Electronic Health Records). Fortunately, this document laid down that sharing any medical data by any (national or international) electronic network must be based on voluntary consent. This document appeared in the last moment, because United Kingdom introduced a medical data sharing network *backbone* that shares personal medical data by the force of the law. Hungary also made an experimental data sharing network that is enforced by the law – i.e. data sharing was done without informing (and consent) of the data subjects.

4.1. Insurance systems shall process medical data within the scope of their activity

The Article 8 of the ECHR enables, that governments may introduce legal provisions in the interests of the *economic welfare* of their nation. This is the mandate of national health insurance systems. In consequence to this, we advise that governments shall remain within this scope of the convention: that means national health insurance systems must not process personal medical data of unsubsidized medical provisions, especially unsubsidized prescriptions' personal data.

4.2. Right to get medical care at freely chosen providers.

We advise that a common European document shall declare, that any patient may seek medical advice, provision of care, or treatment at freely chosen medical providers across Europe independently from the fact that he/she is insured in the national system or not. Costs or part of the costs paid by the patients for the provision of care can be reimbursed according to the national law and the type of the insurance.

From this follows, that any insured patients should have right to get medical provision at private doctors (institutions), in which case the national insurance system must not get information about this treatment.

4.3. Right to get medical advice, physical checkup, elementary lab analysis anonymously.

Taking into account the Article 8 of ECHR, that refers *substantial* public interest we advise that some low cost medical provision shall be given without transferring *personal medical data* (codes of diagnoses and interventions) to the national insurance system. We advise that at least once per year, each insured one must have the right to get medical checkup, elementary lab testing without informing the national health insurance system about his/her medical condition.

We also advise that patients should have right to get this checkup anonymously, that means that even the medical professional, who makes the examination and lab testing shall not collect and store medical data. The findings are ***told*** to the patient, who can keep his hands free, whether he/she wanted to cure his symptoms, where he/she would like to get medical provision and by whom. Such type of medical provision may be provided as a cost based provision, i.e. patients may have to pay for it.

Naturally, in special cases, when a life threatening contagious disease is diagnosed, the anonymity right then shall be ceased according to the national law.

4.4. Pharmacies process medical data for the purposes of accounting subsidization

Pharmacies may process personal medical data of subsidized medical drugs according to national law (or when the drug is a controlled drug, e.g. opiate), and must not process medical data of unsubsidized drugs. We advise, that all insured patients should have right to get drugs full price, without subsidization, which now means that the national health insurance systems cannot get personal data about this prescription.

It is advised, that pharmacies may process personal data about unsubsidized drugs only in the life interests of the patients and on the basis of a written consent.

Pharmacies shall destroy paper based as well as electronic personal data after a retention time according to national law, which should be less than 3 years. As for the paper based prescriptions, we advise that patient name, address, age shall be written on an adhesive leaflet that is removed and destroyed in the pharmacies when expediting the medicine (as seen in the Italian Data Protection Law). Pharmacies can store personal data from the electronic prescriptions according to the above issues. Only unidentifiable financial and statistical data may be collected freely.

4.5. The proportionality of the data processing by the national health insurance systems

The application as well as data retention time of the ICD-10, and medical intervention codes shall be based on the proportionality. Because the purpose of the data processing is the *economic welfare* – this fact shall determine the circumstances of the data processing.

Since many data protection commissioners across Europe declared that ICD-10 codes are disproportionate, (the Hungarian Constitutional Court is also ruled this out) we advise, that a common document shall rule out that medical provisions whose total costs are less than a fixed amount per year (e.g. several hundred Euros) shall be provided without attaching the diagnosis, intervention, doctor, institute code to the accounting data. It may be worth to think, to prohibit the application of ICD-10 codes on the prescriptions on the basis of the above, excepting prescriptions of a *substantially subsidized* medical cure.

It is advised that after some retention time the stored medical data shall be desensitized, the attributes related to personal health (diagnosis, provision/intervention code, institution/doctor code) shall be deleted from the data that will since then contain only financial data – which cannot be considered as sensitive data any longer. The advised period of desensitization is maximum 5 year (according the national law). Financial data can be kept longer, but it is advised to compress them to annual personal costs (without any details) after 10 years.

4.6. The security of the health insurance cards

It is advised, that health insurance cards will not contain the national health insurance numbers but only a card number instead. This can prevent abuses with the lost (stolen) cards, identity thefting and other misuses. Medical service providers need not know what the

national insurance number is. They can account the subsidization on the basis of the insurance card number. When presenting the insurance card, the national insurance clearinghouse would certify the transaction with a transaction number. Medical service providers need not store even the insurance card numbers as it is accustomed when using normal bank credit/debit cards.

We have some suggestions for the medical providers as well.

4.7. Data sharing is based on written and informed consent

According to the 2009/C 128/03 proposal of the EDPS, we also advise that any data sharing across a medical network which contains more than one hospital, clinic, department, ward, pharmacy, ambulance or GP praxis shall be based on written consent. Such network is designed especially for data sharing, that means not only a treating medical professional can access to the data. In that case it is important, who, when and how can access to the medical data of the patients. We oppose such implementation of the electronic prescription system that includes a large national central database where all medical professionals are sending their prescriptions. From the point of data protection only a medical card containing the electronic prescriptions or paper based prescriptions will suit.

4.8. Retention of the paper based medical documents

We consider that medical care providers are allowed to retain personal medical data on the basis of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS-108) Article 9, mainly for the purposes of *suppression of crimes* and on the basis of the 95/46/EC Directive Article 13 (1) d) for *the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions*. The stored medical document will serve as evidence in the trial against the medical providers when a harm or loss of health occurs. We also would like to refer also to the Recommendation R (97) number 5 of the European Commission and the Council of Ministers on the Protection of Medical Data Article 10.

Patients should have right to ask for deletion any unimportant medical data, about temporary diseases, physical assessments, any lab results after 1 year of retention time. Medical laboratories shall delete all personal medical data after maximally 6 months of retention time. (Lab results are given to the hands of patients, who carry them to their doctors or keep themselves.) Medical laboratories must not forward medical data anywhere except when they are authorized by the patient in a written informed consent.

Patients should have right to ask for deletion of any medical data after the legal responsibility ceased, after 1-5 years at a maximum (according to national law). When patients give no provisions, their medical data may be stored for up to 10 years according to an implied consent. After then all data shall be destroyed, excepting when there is a life interest (of the data subject or of their descendants) to store them longer.

4.9. Processing health data at work

We would like to refer to Guidelines concerning the processing of health data in the workplace by Community institutions and bodies issued by the EDPS in September 2009. According to this document, the first screening medical examination shall be restricted to check the minimally needed health condition, and determine whether the employee needs

some aids, special working condition to fulfill his/her task. The yearly preventive screening of the employees is done voluntarily at freely chosen medical service providers.

We would like to advise that the above document together with the similar The Employment Practices Code, Part 4 (by the Information Commissioner of the United Kingdom) shall be strengthened. Both documents lay down that *enforced* application of medical examination in employment shall be restricted to a minimum, when it is absolutely necessary (in the life interests). This is shall be valid for the data processing and data retention as well.

4.10. Secondary uses of medical data

In normal circumstances medical service providers may use medical data for administration purposes according to 95/46/EC Article 8 (3). This can be done only if confidentiality is maintained. We argue that if during the administration of a health institution the absolute confidentiality cannot be ensured, i.e. other medical professionals who were not treated the data subject may access to his/her medical data, then a written informed consent given by the patient is indispensable.

We also advise, that if any secondary use of medical data (biological sample, tissue) is foreseeable (for the purposes of teaching, research, publication, transfer etc.), then data subject shall be informed about these at the time of admission the latest. The data subject then should declare in writing whether he/she is consented with the secondary use of data.

Data subjects may block to use any of the medical data relating to him/her, without indication of the reasons. In that case data may be processed only for national security and crime prevention purposes. If blocking harms life interests of the data subject's family, then they shall be informed about these circumstances beforehand. Data subjects may require that after the legal retention time is elapsed their data is to be deleted automatically.

4.11. The data processing after the death

After the death of the patient all unimportant medical data shall be deleted right then. Important personal medical data that may have connection to the cause of the death shall be deleted as the legal responsibility ceases. Data shall be communicated to the descendants (family) of the data subject if this is in their life interests before deleting the data.

4.12. Penalizing breaking medical confidentiality

It is advised that breaking the law of medical confidentiality should be penalized by up to 1-2 years of imprisonment. If minimal breach occurs then the guilty medical professional shall be fined up to 2000-20.000 Euros.

4.13. Prohibition of long term archiving

According to the ETS-108 convention, personal medical data keeping stored in a national archive shall be prohibited. We argue that forwarding personal medical data to a national health archive shall be based on the written informed consent given by not only the data subject but all of his family members. The reason is that data remains related to the family members even after the death of the data subjects. Much health related sensitive information can be inferred from these data that may substantially harm the interests of the still living descendants. If data subject have no descendants, that he/she alone may give informed consent to forward personal data to a medical archive. According to the Ovideo Treaty his/her intention must be respected.

5. Data processing for scientific research

The autonomy of the data subject within scientific, especially in medical research is a long existing question. After the WW2 it seemed that medical community put his coin to the voluntary consent, see the Nürnberg Code. Later it was strengthened in the Helsinki Declaration of the World Medical Association and in the Ovideo Treaty (CETS-164) in 1997.

On the other hand this trend was changed. In 2008 the Medical Academy of the United Kingdom opens a front against voluntary participation and they pressed the World Medical Association to amend the Helsinki Declaration so that, some time the interest of a medical research is more valuable than the personal interest of being left alone – this way of thinking is mirrored in the establishment of the NHS SUS (Secondary Use Services), which made some data available for business purposes collected by the National Health Service without consent of the data subjects. The SUS database contains identifiable *personal* health data, but it is claimed that the service provides registered users only aggregated statistical data. Meanwhile people do not know whoever can access to the detailed, itemized data.

We would like advise to declare that medical (and other sort of) research that makes use of personal data shall principally be based on *voluntary* consent. The most important personal right is the *right for living*, and the second should be the right to *human dignity*. From this point of view, a repressing (enforced) research that reveals medical details from somebody to others shall be inhuman trespassing upon data subject's dignity. In certain rare cases personal data still can be used for research when obtaining consent is impossible or needs disproportional effort. This somehow follows from the EU data protection principles. On the other hand it is advised to keep in mind the words of the former data protection commissioner of UK (Elizabeth France), who said that sending a postal mail to the patient to obtain his/her consent *is not disproportionate*.

5.1. When personal data can be considered anonymous?

Many times scientific research does not need personal data. Researchers openly declaring that they will not use any personal data. They remove names, address and health insurance number from the data claiming that the remaining data is anonymous. Are they right? Absolutely are not.

Let us make a mind experiment. For the purposes we are an employer and would like to get medical information about someone who has been absent on a certain date and presenting a medical certification. The certification contains no medical information only the medical professional's name and code, the date, the age and gender of the patient (employee). It is astonishing that he/she can be looked up in the "anonymous" database by the date and doctor's name (code), age and gender uniquely. From such a database then we can obtain detailed medical information about anyone. This means, that removing natural identifiers from the data does not mean, that the data becomes anonymous – it is also written in the Working Paper 136 of the 29 Working Group on Data Protection, on the concept of personal data.

Many times researchers want to work with time series. These are containing lists of medical events (examinations, interventions) related to certain patients. Time series are especially dangerous for the privacy of the patients, because data can be identified by taking only 2-3 dates from the health history. From this follows that any time series that contain exact (daily) dates can never be considered as anonymous.

It is advised that the concept of anonymity should be clearly and rigorously defined. The US Health Ministry elaborated a guideline (see HIPAA guideline) that deals with anonymization. It summarizes those kinds of data items that should be deleted during anonymization minimally. Introduction of such a guideline and education would be very important in the health sector, where the privacy of the data subjects should be ultimately preserved.

Elaborating an anonymity testing method, by which ethics committees and medical researches may assess the risk of breaking the confidentiality, is also advised.

5.2. Cancer Registries

We would like to advise that a common European data collection and protection protocol shall be elaborated. The most favorable method is the French or German, where patients may get to know what sort of data is to be sent and may object against sending his/her personal identification data. The collected data items, the retention time, handling data after death, the publicly available access protocol to the data, the publicity of the research approved by an *independent* ethics committee all calls for a common ruling that shall take into account data protection principles.

Following the above way of thinking, we advise that after the death of the data subject all data shall be deleted. The descendants of the data subject shall be informed about the stored data if it is in their life interest beforehand.

5.3. Scientific research on special categories of personal data

It is advised that any scientific research that deals with special categories of personal data should get similar protection as health data. It is advised that an *independent* ethics committee should revise the research plan, an independent authority shall give permission for the research, and data subjects should give written consent to allow using his/her sensitive data. This shall concern to research on personal criminal data, on personal data which relates to religion, world view, membership of trade unions, membership of political parties, societal organizations etc.

5.4. Genetic research and examination

The genetic research shall be done on the basis of voluntary consent. Research must not be done on those human beings who cannot give their consent, especially on children. This naturally means that personal genetic data must not be collected from those people who are not able to give informed consent.

Genetic examination can be done in the life interest of patients on the basis of written informed consent. When genetic examination is initiated by the parents of a child, it shall be done only when it is in the life interest of that child. When this child reaches the adulthood, it should be offered him/her to destroy the obtained genetic information (and sample) with or without communicating the finding. He/She may want to know the information or may want not know it, the decision must be respected. The now adult patient may also decide to give written consent to further storage of his/her genetic sample and data.

5.5. Medical research done by governing bodies

When medical research is done by the bodies of the health government or the health insurance system, this shall be done according to the existing law. It is advised, that a common European document should give a clear distinction between administration and research tasks. See: Committee on the Role of Institutional Review Boards in Health Services, Research Data

Privacy Protection, Division of Health Care Services, Institute of Medicine: Protecting Data Privacy in Health Services Research, National Academies Press US, pp. 11. ISBN: 0-309-56486-7, (2000).

This means that the research plan shall be evaluated by an independent ethics committee and a written consent from the data subjects shall be obtained. We advise that the opinion of the ethical evaluation put out on the internet, as well as the description of the research. The organization of the research should take into consideration if some people do not want to participate. A period should be provided, during which data subjects may block their data, i.e. prohibit being used in the research.

6. The preliminary data processing explanation

Although preliminary data protection information is widely given to data subjects, there still exist such organizations in member states who fail to provide such information (e.g. in Hungarian healthcare).

6.1. Sanctions against data processors who fail to give preliminary explanation

Since the requirement of giving preliminary data protection information is rather old (20 years old at least). We would like strengthen that all ***personal data processors*** must provide such information by themselves or by their representatives. Whenever a data processor fails to provide such information (on the internet, or in writing when first meets the data subject) then they shall be fined 1000-100.000 Euros. Centralized national organizations shall be fined even more severely.

7. The rights of the data subject

In some cases personal data is collected unlawfully but this reveals later. When a new database containing personal data is established, governments make a law that controls the collection of the data. Later defenders of civil rights or data protection activists may attack the law before the constitutional court. If the constitutional court decides in favor of the civil activists, it deletes parts of the attacked law, but the data remains at the hands of the data processor.

7.1. Right to delete data when there is no legitimate interest for storing data longer

We would like to urge, that a common European document shall rule out, that any database (or part of the database) that later proved to be unlawful by the decision of a European body or a national constitutional court shall right then be destroyed within 30 days. If a government organization fails to destroy the database (or a part of it) any citizen may apply first to the national data protection commissioner, if he/she fails to act within 30 days, then to a dedicated European body, who initiates investigation against this member state.

8. National archives

It is advised that the special categories of personal data shall not be stored in national archives, excepting those cases when data subject (and their family, if exists) gives written consent to it.

8.1. Special categories of personal data

We mentioned in the 1.2. that the data collected in the interests of the national security shall be declared as special, sensitive personal data. If we accept this, no secretly collected personal data could end up in a national archive.

In the Eastern and Central Europe the question of secret documents collected by the previous political system is still important. Possibly a correct and satisfying decision cannot be made. Either all documents can be destroyed, or all documents can be given to the data subjects (who have been followed, have been spied after them by secret agents) or all data should be made publicly available. Perhaps, the documents shall be given to the hands of the data subjects, who then can decide what they would like to do with them. Storing further these sensitive personal documents without providing the right for the deletion of the unlawfully collected data is the worst that one can do.

9. Immunity of special categories of personal data

As we already mentioned, we would like to advise some sort of immunity for special categories of personal data, especially for personal health data. Generally, we accept the right of the society to fight against crime and terrorism. Even then, we argue that national security and crime prevention can be maintained with other types of personal data. There are plenty of them: credit card details, video surveillance data, travel information, internet traffic, mobile or land phone traffic data etc. It should be enough.

9.1. Special categories of personal data

We advise that medical data shall be given immunity. That means that police and national security organizations may require personal health data if it is necessary for preventing a mass catastrophe like hijacking an airplane, bombing in a shopping center i.e. in the life interests of others, for other purposes not. The data shall be deleted as soon as is not necessary for the original purposes of the collection e.g. the terrorists have been captured.

10. Other questions

10.1 Right of access

Any authorized or lawful access to personal data including that of the person concerned is in good order. Nevertheless the unauthorized access, followed by the misuse of personal data, if it comes to the knowledge of the competent authorities, should not only be penalized, but the person concerned should also be informed about it. It is then up to him, to decide what measures he takes against the person infringing his rights.

10.2. Automated individual decisions

Decisions made exclusively by automated processing of personal data (eg. Voice Risk Analysis) used make judgment on the creditworthiness or as pre-employment test should rely first of all on the voluntary and informed consent of the person concerned, which consent should be revocable during or after the processing without any detrimental effect. According to the professional literature these automatic means are not fully reliable. Therefore when the automated decision is not favorable for the person concerned, a tradional method should be implemented.

10.3. Security of processing

The very broad concept of security obliging the data controller to "implement appropriate technical and organizational measures" against any unlawful activities aiming at the intrusion into personal data files is no longer satisfactory. The data controller or processor should have the legal obligation to implement privacy enhancing or tamper resistant technologies as well as those defined by international standards.

Budapest, 30 December 2009.

In the name of the association

Dr. Zoltán Alexin, PhD.
senior lecturer
University of Szeged,
H-6720
Árpád tér 2.
Szeged, Hungary
e-mail: alexin@inf.u-szeged.hu
web: http://www.inf.u-szeged.hu/~alexin

Dr. Pál Könyves Tóth
lecturer
Pázmány Péter Catholic University
H-1088
Szentkirályi u. 28-30.
Budapest, Hungary
e-mail: kotopa@jak.ppke.hu

Member of the Scientific Advisory Committee
of the
European Privacy Institute