Legal Discussions in Data Privacy and the Environment in Bosnia-Herzegovina

Husic SAMİR
PhD candidate
International University of Sarajevo
Bosnia and Herzegovina
samirhusic@gmail.com

Ozguven KUTLUK
Assoc. Prof. Dr.
International University of Sarajevo
Bosnia and Herzegovina
kutluko@yahoo.co.uk

Abstract: Dramatic increase in importance of data privacy came with advance of information technology. Global domination of information exchange is forcing governments to establish international standards and regulatory mechanisms in order to protect data privacy. These efforts resulted in general principles of data privacy, which have been widely accepted, but also difficulty for diverse legislations.
While Europe has highly developed and human rights oriented data privacy regulations, USA has less regulated and business enhancing oriented approach. Such discrepancy resulted in continious international discussions and agreements towards regulation's harmonization.
Data privacy regulations in BiH has radical boost recently. The main push was protection of data privacy as condition for visa liberalization with EU countries, making BiH data privacy in full compliance with EU standards. However, when it comes to practical application, there's significant amount of data privacy interference and lack of awareness, while most serious breaches are conducted by public administration.

Introduction

The main challenge in personal data privacy is to share data, particularly in respect of freedom of information principles, while protecting personally identifiable information. Personally Identifiable Information („PII") is a unique piece of data or indicator that can be used to identify, locate, or contact a specific individual (Staples, 2007, pp.383-386). What distinguish PII from other types of personal information is permission of identification by this information, as it may be sensitive, embarrassing or offensive in a way that individual may wish to keep it private.

Data privacy issues can arise in response to a wide range of PII, including an individual's name; geographic, physical, or postal address; phone number; electronic mail address; bank or credit account numbers; and Social Security number. Some information can be collected anonymously, like state of residence, age, gender, race, purchases, or salary. However, personal information from various sources can be pieced together to create PII. For example, an Internet Protocol address does not, by itself, identify a specific person. But when combined with an Internet service provider's customer records, the combined information becomes PII (Staples, 2007).

Remarkable increase in personal data privacy importance came with the advance of information technology. The information is collected, stored, and shared by individuals, organizations, but also government institutions. Exchange of personal data became necessary to enable or develop many activities, to communicate, obtain benefits or transact business. With such striking increase in importance, the issue became equally complex from legal point of view, because of different definitions of "personal information" in different legal context. It is impossible today to collaborate with stakeholders in a foreign country without appreciation of complex regulations regarding data rights. Global technology, communications and outsourcing made it crucially needed to arrange regulatory mechanisms internationally.

The legal protection of the right to privacy in general, and of data privacy in particular, varies greatly around the world. There is a significant challenge for organizations that hold sensitive data to achieve and maintain compliance with so many regulations that have relevance to information privacy. A lot of attempts are made to regulate privacy issues internationally that would be obligatory and acceptable for different countries. Those attempts to create universal principles of data privacy can be traced even before contemporary global data exchange challenges.

The root for international standards in data privacy may be found in The Universal Declaration of Human Rights. It is adopted by the United Nations General Assembly in 1948 in Paris, and it reflects the consequences of Second World War. It consists of 30 articles which have been foundation for further international and national regulations. In the Article 12, Declaration define right to privacy, and unlike later privacy regulations, it prescribe no exception: *"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks."* (General Assembly of the UN, 1948)

But only in early 1970ties, government agencies in the United States and Europe have studied the manner in which entities collect and use personal information, their information practices and safeguards required to ensure adequate privacy protection. The result has been series of reports and regulations, while common to all are five core principles of privacy protection (Federal Trade Commission, 2007). These principles were first articulated in the United States Department of Health, Education and Welfare's report entitled *Records, Computers and the Rights of Citizens* (Secretary's Advisory Committee, 1973). The five principles are:

1. Notice/Awareness - persons should be given notice of an entity's information practices before any personal information is collected from them.
2. Choice/Consent – persons should have options as to how any personal information collected from them may be used.
3. Access/Participation – person should have ability both to access data about him or herself, and to contest that data's accuracy and completeness.
4. Integrity/Security – data has to be accurate and secure.
5. Enforcement/Redress – there must be a mechanism in place to enforce the core principles of privacy protection.

These principles are widely accepted at that time, and influenced data privacy legislation in following 30 years. Yet, these principles later have been criticized for being short and incomplete, allowing too many exemptions, and not keeping pace with information technology. There are numerous comprehensive data privacy principles developed later on, and most influential are contained in OECD Guidelines on the Protection of Privacy (OECD, 1980), and EU Directive.

Data Privacy in Europe

Data privacy regulation has relatively long tradition, and it is generally considered to be strict and highly developed in EU. Its roots could be found in the European Convention on Human Rights from 1950. ECHR Convention is signed by 47 member states of the Council of Europe ("CoE"), and one of them is BiH which signed and ratified it in 2002 (CoE, 1950). It sets forth a number of fundamental rights and freedoms, including right to respect private life, prescribed in Article 8. Member states undertake the responsibility to ensure these rights and freedoms to everyone within their jurisdiction, and the ECHR Convention establishes an international enforcement mechanism.

European Court for Human Rights uses a very broad interpretation of this Article 8 in practice. It provides a right to respect for one's "private and family life, his home and his correspondence", subject to certain restrictions that are "in accordance with law" and "necessary in a democratic society". It may be compared to the jurisprudence of the United States Supreme Court, which also adopted broad interpretation of the right to privacy in protecting private and family life. For example, very appealing modern-day issue of employee's privacy is judged in 2007 under Article 8 in case of Copland v. The United Kingdom (ECHR, 2007). In this case, ECHR found that UK had violated rights of privacy and correspondence of complainant, by the way of monitoring and keeping data of her telephone calls, e-mail correspondence and internet use. Employer, a state-administered body, under deputy principal request, monitored complainant's telephone, internet and e-mail use in order to discover whether she was making excessive personal use of them.

In 1976, the Committee of Ministers recognizes the need for international binding agreement regarding data protection (CoE, 1981). This Committee recommended preparation of a convention for the protection of privacy in relation to data processing abroad and trans-frontier data processing, which finally resulted in CoE conclusion of

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data in 1981 ("Convention"). Accordingly, this Convention is created due to need for international agreement in law application when automatic processing of personal data involves parties in different countries, for example usage of bank terminals in other countries. International mechanism have been necessary, having regard to rapid evolution of personal information handling at that time, so the states can inform and consult each other on matters of data protection.

This Convention is the first binding international instrument which protects the individual against abuses caused by the collection and processing of personal data, and also regulates trans-frontier flow of personal data. It prohibits the processing of sensitive data, such as person's race, politics, health, religion, sexual life, criminal record. Restrictions on the rights prescribed in Convention are only possible when prevailing general interest is at stake, such as state security (CoE, 1981). This Convention obliges the signatories to enact legislation concerning the automatic processing of personal data, and it is signed and ratified by 41 member states of CoE.

In 1995, European Commission, being still concerned with diverging data protection legislation, decided to harmonize it by proposing Directive 95/46/EC. To move toward harmonization, the European Parliament and CoE issued the Directive on the Protection of Personal Data ("Directive") (CoE, 1995). This Directive became the backbone of the current EU data privacy legislation. Directive is not legally binding for citizens, but rather member states have to transpose it into domestic law. As a result, EU member states incorporated it into domestic laws by the end of 1998, and established supervisory authorities to monitor level of privacy protection. For example, UK enacted Data Protection Act 1998 to bring UK law into line with the Directive, and this is the main act that governs data privacy protection in the UK (Information Commissioner's Office, 1998).

The Directive aims to protect the rights and freedoms of persons with respect to the processing of personal data by prescribing guidelines for domestic legislation. These guidelines define when private data processing is lawful (CoE, 1995). Beside guidelines, it provided important list the eight enforceable principles of good practice for processing personal data (Information Commissioner's Office, 1998). Briefly, these principles, that every member state must comply with, specify that personal data must be:

1. Processed fairly and lawfully.
2. Obtained for specified and lawful purposes.
3. Adequate, relevant and not excessive.
4. Accurate and up to date.
5. Not kept any longer than necessary.
6. Processed in accordance with the "data subject's" (the individual's) rights.
7. Securely kept.
8. Not transferred to any other country without adequate protection.

Although the Directive offered most developed and world widely accepted data privacy standards today, recent study shows that it became outdated. The UK Information Commissioner's Office announced report in May 2009, stating growing fear that the current Directive is outdated and too bureaucratic. It says that Directive is often seen as burdensome and too prescriptive, and may not sufficiently address the risk to individuals' personal information (Robinson et al., 2009). Similar evaluation is given on the 4th annual Data Protection day in January 2010, calling for reform of the Directive (Reding, 2010). Concerns are raised by new challenges, such as behavioral advertising by using internet history, social networking sites, and smart chips used for tracing. It warns that data protection rules must be updated to keep abreast of technological change to ensure the right to privacy, legal certainty for industry, and the take-up of new technologies.

Data Privacy in USA

Data privacy regulations in United States are not highly regulated. USA use a so called "sectoral" approach that relies on a combination of legislation, regulations, and self-regulation, but there is no all-encompassing law regulating processing and storage of personal data, comparable to EU Directive. These regulations, industry best practices and other binding structures have been enacted at the federal, state and even local level. They pertain to a variety of matters, like financial information, video rentals, electronic communications, or healthcare information. As a result, it is certain that one or more privacy law or regulation, local, state, or federal, does affect and govern some portion of many companies' activities (Gilbert, 2003).

US data privacy legislation tends to favor information flow efficiency, rather than individual rights to control over their own personal data. The reasons for such approach have to do with American "laissez-faire" economics, which allows industry to be free from state interventions and restrictions. Another reason is constitutional

right of free speech guaranteed in the First Amendment, providing broad interpretation in regard of information open flow.

Historically, the legal requirements of privacy legislation in USA had slow development. Some of the first legal discussions started in 1890, when Louis Brandeis and Samuel Warren published the article "The Right to Privacy" in the Harvard Law Review (Staples, 2007). However, regulations started increasing in frequency only since beginning of 1970ties. Additional impulse they got in late 1990ties, the time of EU Directive incorporation in European countries' legislation.

There is a list of more than 40 privacy-related laws in USA, only on federal level, while each state has its own privacy-related laws and regulations (Herold, 2002, p.529). Some of the most important are: Fair Credit Reporting Act (1970), Privacy Act (1974), Family Educational Rights and Privacy Act (1974), Right to Financial Privacy Act (1978), Electronic Communications Privacy Act (1986), Telecommunications Act (1996), Children's Online Privacy Protection Act (1999), Health Insurance Portability and Accountability Act (1996), etc.

This complexity in US data privacy regulation, and having no comprehensive act on data privacy protection, became a barrier to US business with EU countries upon adoption of EU directive. As mentioned above, The EU Directive prohibits the transfer of personal data to non-EU countries if it doesn't meet the "adequacy" standard of privacy protection, except in the cases of the derogations listed (CoE, 1995). Accordingly, it created a legal risk to organizations which transfer personal data from Europe to the US. Although US share the same goal of enhancing privacy protection for its citizens, the US took different approach to privacy from that taken by EU. In order to bridge these different approaches, and to simplify means for US organizations to comply with Directive, the US Department of Commerce in consultation with the European Commission developed a "Safe Harbor" framework (Safe Harbor, 2000).

"Safe Harbor" Framework

EU Directive barred the transfer of personal data from EU citizens to businesses and other entities in countries without levels of privacy protection estimated as "adequate" by the EU. Thus, the Directive sets de facto standards for data protection internationally. Accordingly, countries such as Canada, Australia, and Japan have implemented data protection laws that provide similar levels of protection for personal data. But the United States find it difficult, and rather have worked out special agreements with the EU so that US businesses can claim compliance with these principles (Staples, 2007, p.209). Such principles are supposed to simplify relations between US and EU businesses.

At the time of EU Directive adoption, the prevailing American response reflected in denial. Dominant American belief was that European data privacy protection may disturb American interests in privacy protection policy that is consistent with its constitutional framework, free speech philosophy and deregulated market economy. At that time, some US critics proposed resistance to Directive, while others tried to prove that combination of sectoral legislation amounts to "adequate" level of data protection. Still, general opinion was that the implementation of the Directive will produce confrontation over the "adequate" context of data protection. While concerned with interest of US business with EU countries, they believe that EU have to decide whether purpose of Directive is to protect European citizens from processing their data abroad, or to promote adoption of equivalent data protection law around the world (Bennett & Raab, 1997).

Because the US has no privacy legislation of general applicability, to help US companies comply with the EU privacy laws, the US Department of Commerce has implemented an International Safe Harbor certification program. It is approved as adequate providing protection of personal data by the European Commission in July 2000. The Safe Harbor addresses data privacy issue in unique way as voluntary program, rather than law imposed to all organizations. A US company that adheres to the Safe Harbor Principles and complete certification program, receive presumption from EU member states that it provide required level of personal data privacy protection (Gilbert, 2003). If dispute arise in relation to data transfer according to Safe Harbor program, it is ultimately resolved at European Data Protection Authorities Panel.

Although it is reached as best possible solution, Safe Harbor program agreed between US and EU raised numerous issues. First of all, it is failing to balance fair interest in data privacy. This program allows that US companies abided by its provision afforded more privacy protection to Europeans than Americans under US laws. It seems that this agreement might prompt the US to shift its privacy policy in accordance with European standards, which views personal privacy as "human" right. The US failure to enact privacy legislation of general applicability can be considered as continuing characterization of personal data privacy as "consumer" rights issue, rather than "human" rights (Brown & Blevins, 2002, p.565). Beside this issue of not balanced privacy rights, Safe Harbor has other complex issues like when personal data is transferred from EU to US, and then to third countries. Also,

participation in the Safe Harbor program has no effect on compliance with the requirements of privacy laws outside the EU area. Consequently, being not complete solution, Safe Harbor became a model for other controversial programs, like the "U.S. – Swiss Safe Harbor" (Safe Harbor, 2000), and other bilateral agreements regarding personal data privacy between US and European countries.

Bosnia and Herzegovina Regulations Regarding Data Privacy

Development and implementation of rules and regulations in field of data privacy is considered as a very important step for BiH in terms of compliance with EU standards. With this orientation, the Law on Protection of Personal Data ("Law") became the foundation and marked new age of data privacy legislation in BiH. It prescribes establishment of supervisory agency and number of regulations, all in accordance to EU Directive.

The Law prescribes, first of all, that no one has the right to handle personal data of citizens without their consent or a valid legal basis. The other principles of Directive are respected in Law, like the purpose of taking personal data, and timely and accurate processing of personal data. Also, every citizen must be informed that his personal data is being processed.

According to Law, BiH's Data Protection Agency ("Agency") is established as supervisory authority and has become operational and begun its work in June 2008. Its key tasks are to supervise the implementation of the Law on Personal Data Protection; to investigate complaints by the public about possible breaches of data protection regulations; to order blocking, erasing or destroying of data, issue temporary or permanent bans of processing, issue warnings or reprimands to the controllers; to organize training and raise the awareness of government institutions as well as the wider public about data protection obligations; to provide advice and guidance on data protection matters; carry out inspections of government institutions to check whether they comply with the rules of data protection; and to ensure that no legislation infringes with the protection of personal data (Law on Protection of Personal Data, 2006).

Beside Law, there are four book of rules enacted in 2009 (Official Gazette, 2009) supporting this Law. They are: Rules on the manner of keeping the records of personal data filing systems and the pertinent records form; Rules on the manner of keeping and special measures of personal data technical protection; Regulation on supervision inspection regarding protection of personal data; and, Regulation on procedure upon complaint by the data subject filed to the agency for personal data protection. Director of Agency also issued the Instruction on how to verify the processing of personal data before the establishment of collection of personal data.

Regarding international regulations, worth to mention is a short list, defined by the Agency, of five most important international regulations applied on data privacy legislation and practice in BiH. These regulations are explained briefly in above part regarding European data privacy legislation. The key international sources for BiH data privacy legislation are: European Convention on Human Rights and Fundamental Freedoms, adopted by BiH in 1999; Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, together with additional protocols entered into force in BiH in 2006; and Directive 95/46/EC, transposed in BiH Law on personal data protection in 2006.

Beside these, BiH adopted Directive 2002/58/EC in 2002, at the same time when new legislative framework designed to regulate the electronic communication sector. It is known as Directive on Privacy and electronic communications, and contains provisions on a number of sensitive topics, such as the keeping connection data for the purposes of police surveillance, the sending of unsolicited e-mail, the use of cookies and the inclusion of personal data in public directories (Directive on privacy, 2002). It also known as E-privacy Directive, as it mainly regulates important privacy issues in digital age, such as confidentiality of information, treatment of traffic data, spam and cookies (E-Privacy Directive, 2003). BiH also adopted Recommendation No. 15 and addition on Committee recommendation regulating the use of personal data in the police sector. The CoE Committee of Ministers recommends with it that the governments of Member States respect a series of principles concerning control and data collection, notification of automated files, storage, use and communication of data for police purposes, and rights of access, rectification and appeal to police files (CoE, 1987).

Data Privacy Protection as Condition for BiH Visa Liberalization

Most important factor that influenced data privacy environment in last 5 years obviously was condition to join EU. One of publicly most talked benefits of joining EU is freedom of travel, which more specifically means visa liberalization. Very hard and expensive ways of obtaining visa for most countries in the world have been frustration for BiH citizens almost 20 years. Getting advantage of traveling in EU without visa would certainly mean victory equal to becoming an actual EU member state.

BiH signed Stabilization and Association Agreement in June 2008 with European Communities and their member states, where Article 79 is dedicated to protection of personal data. This Article prescribe that "Bosnia and Herzegovina shall harmonize its legislation concerning personal data protection with Community law and other European and international legislation on privacy upon the entry into force of this Agreement. Bosnia and Herzegovina shall establish independent supervisory bodies with sufficient financial and human resources in order to efficiently monitor and guarantee the enforcement of national personal data protection legislation." (Stabilization and Association Agreement, 2008).

One of the key conditions for BiH visa liberation is securing full respect for fundamental principles of data protection. This has been emphasized since Law on Personal Data Protection has been enacted in June 2006, and it has been driving force for drafting data privacy legislation until today. Seminars and trainings have been conducted since then, supported by European Commission and including European trainers, as it was not be realistic to expect visa liberalization regime without paying due attention to this issue. Project supporting Commission for BiH Data Protection, existed at that time, prepared seminars for specific sectors, like police, bank, health and telecommunications, but also public campaign.

Enactment of the Law by the BiH Parliamentary Assembly has provided full compliance and implementation of European standards in the area of respect for fundamental human rights and freedoms, particularly the right to privacy. The Law also prescribed the establishment of the Agency, which should be engaged in supervision over the enforcement of Law and respect for privacy rights regarding breaches of personal data. However, although planned to be established immediately, the Agency started to function only in June 2008 (Kazagic, 2009). It had only three employees, director with two associates, until beginning of 2009. By the beginning of 2010, agency works still with insufficient capacities, and has only 16 employees, although Book of Rules on Internal Organization prescribed 45 employees (About the Agency, 2010).

As additional indication of importance of data privacy protection for European integration process, there is a fact that Director of Agency, Petar Kovacevic, have been appointed as member of workgroup for liberalization of visa regime. The task of this group is working on requirements fulfillment of the recently presented the Roadmap, which including preparation of action plans of the Roadmap sections (Sjednica Vijeća Ministara, 2009). According to September 2009 report of this workgroup for liberalization of visa regime, Personal Data Protection Agency is fully functional, while regulations on personal data protection are fully implemented (Interresorna radna grupa, 2009).

The European Union show significant interest in increasing the level of data protection, especially in the sector of the police forces in BiH. In this regard, it has provided 250,000 Euros for the project "Support to the Personal Data Protection Agency of BiH". The project lasted from October 2009 to march 2010, and it is implemented by Personal Data Protection Agency Saxony in cooperation with BiH Agency. The project consisted of three activities: legislation analysis and harmonization of personal data protection legislation in accordance with the EU Standards; strengthening of institutional and human resources capacities of the Agency in order to enable it to fulfill its competencies; strengthening of awareness and capacities of public institutions processing personal data (European Union, 2009). This project, implemented by experts from Germany and Slovenia, has been evaluated as highly successful by EU Delegation in BiH. The result of the project is that legislation in the field of protection of personal data has been brought into full compliance with relevant EU standards (EU će budno pratiti, 2010).

However, there are recently expressed diverse opinions about functionality of private data protection system in BiH. European Commission presented BiH with an updated assessment of the Roadmap implementation for visa liberalization in June 2009. It states, in part regarding personal data protection, that two tasks are still needed:

- Measures to make the Data Protection Agency fully operational
- Measures taken to ensure the implementation of the rules for personal data protection (European Commission, 2009).

Even in the latest assessment (European Commission, 2010, p.35) of Bosnia and Herzegovina, Commission concludes again that no fully operational independent Data Protection Agency has been put in place yet, even though Director of the Agency was appointed in June 2008. Main critics have been directed to adoption of additional required by-laws, and ensuring implementation of the Law in all relevant areas.

Having in mind these opposing views, the head of the EU Delegation in BiH, Dimitris Kurkulas, said recently that the EU will very closely monitor compliance with data protection in BiH, especially when it comes to liberalizing the visa regime (EU će budno pratiti, 2010). He emphasized importance of future cooperation in the international field in the area of data protection and information sharing, which requires the need to respect the rules and regulations concerning the protection of personal data.

Lack of Citizen's Awareness of Data Misuse

Misuse of personal data in BiH is notable for years. Each registration is risky, as usually there is no guarantee of privacy, or it is written in small letters that they have claim to your information. Data can be used only for the purpose for which they were collected, but those who collect data are not sufficiently aware of their legal obligations and keep them longer than they should.

Every citizen in BiH has the right to submit a complaint to the Agency when one learns or suspects that one's personal data is unlawfully processed. There are complaints, but unfortunately, the awareness of citizens regarding personal data protection, and rights that derive from it, are on the same low level as before Law was enacted. There have been only ten complaints of citizens against data privacy violation until December 2009 (Kazagic, 2009). Agency is working on a campaign to improve this situation, and most evident was their campaign in late 2009 and beginning of 2010, when project of EU supporting development of Agency was implemented.

Citizens of BiH are very often required to provide private data, from shopping centers to public institutions, and they get not used to resist it. Although citizens don't have sufficient awareness, still, those who demand their personal data are responsible for seeking and processing such data. Data collectors may use data only for the purpose for which it is collected, but arbitrary use of personal data exist. For example, citizens are forced to give a Unique Identification Number (UIN) for almost every little thing, and almost every paper form require this information. UIN is also called Unique Master Citizen Number, and it has similar purpose like Social Security Number in USA.

Law on UIN precisely prescribe who can use this number, for what purpose, and if consent of citizen is required. It is interesting that Law on UIN listed BiH institutions of local government and entities having the right to use a UIN, but does not mention public companies, banks or shops, who usually request this number from citizens when payment is arranged in rates. ID card may be given for identification purpose, but prescribing or copying UIN number from ID card is against the law. This is why Agency requested modifying Law on Identity Card, and to prohibit from using copies.

BiH Public Administration

The recent information shows that public institutions are those who mostly undermine the right of BiH citizens on data privacy (Agencija zatražila, 2010). BiH legislation emphasize that personal data must be private property, and no public institution should use it without explicit permission in law. But in BiH practice it happens to be different. There are numerous cases of using personal data without required permission of citizen. Although Law exists for years, they behave against Law when it comes to dealing with citizens' UIN.

Even further, more than three years from the enactment of Law in 2006, most of public institutions still didn't adopted sublegal regulations required by this Law. Public institutions are required, according to Article 11 of the Law, to adopt Book of Rules for Processing Personal Data, and Plan for Protection of Personal Data. Although there are penalty provisions, most public authorities failed to comply with the Law in this regard. It is assumed that legacy of the past political system made public authorities believe that they own and control data, including personal. Agency intends to protect citizens from these practices. They already initiated process to amend the Law on ID card, to include prohibition from using the copy of card, where possibilities of identity theft are noticeable (Krsman, 2009a).

As further step, Agency recently announced implementation of misdemeanor warrants in order collecting fines that may go up to 100.000 KM. Most serious violations prescribed by Law are related to the processing and transfer of personal data into foreign countries, and such practice exist in BiH. Penalties are provided for violating the Law, and the Agency is still working on integrating into "Sanctions Registry", which is precondition for imposing sanctions. No sanctions are imposed yet, although Law is enacted about 4 years ago, and violators are not penalized so far.

First activities of the Agency have been focused on establishing functional inspection, and some urgent inspection control has been conducted in June 2009 over 20 public institutions, including police agencies and Ministry of Foreign Affairs. The condition of data privacy protection has been evaluated as "unacceptable" (Kazagic, 2009) and certain public companies have been ordered to destroy databases of citizens' UIN's because they have no right to collect and keep such data.

The next steps in 2010 in ensuring of data privacy are again focused on public administration and public companies. Agency has planned to establish main register with information about all databases containing private data in BiH public administration (Krsman, 2009a).

BiH Data Privacy Cases

Agency found out that most common deficiencies in the processing of personal data are inherited practices, a lack of knowledge about regulations, lack of rules and procedures, and lack of plans for the protection of personal data (Institucije BiH, 2009). Following four cases reflect the data privacy protection deficiencies in BiH environment. All cases involve public administration or public enterprises.

1. When seeking the license for possession of the weapon in Sarajevo, a citizen come to Ministry of Interior (MoI) and apply, and then he is directed to next office where he is requested to bring Police Clearance Certificate. He is supposed to pay for obtaining this Certificate. However, Certificate is issued by MoI, same ministry that requested him to obtain the Certificate. Obviously, they could obtain requested data in ex-officio procedure, rather than requesting it from a citizen. And not just that citizen is obliged to seek from MoI and provide to MoI certificate about personal information, but also he has to pay 35KM tax for this data processing. Agency is of opinion that this practice must discontinue, and that determination of tax is not according to law (Krsman, 2009a).

2. Agency received a number of citizens' complaints that their unique identification numbers (UIN) and other confidential information are exposed to public eyes by Public Enterprise "Elektroprivreda". The problem is raised more than year after Law is enacted, when citizens recognized illegally presented private data on their electricity bills. These bills are left in (or nearby) mailboxes in hallway of building, and they are not in envelopes, so every neighbor can read private data contained on bill. Irregular payers of utilities are sometimes listed on special notice in building hallway. This case ended by Decision of the Agency, dated 8th May 2009, that orders Elektroprivreda blocking and deletion of personal data (UIN) of electricity consumers. Elektroprivreda denied possibility of personal data abuse, even though they possess personally identifiable information (Krsman, 2009b). Rather than use of UIN, Agency advised public enterprises to use consumer codes. Public companies meanwhile changed the system of printing bills, and discontinued printing UIN.

3. Sarajevogas Company, main natural gas distributor, has similar disputable system of personal data processing like Elektroprivreda. Although they deny possibility of abuse, it is easy to obtain personal data of costumer by simply typing customer code on their website. This code is contained on customer's bill, often unprotected in residents' building hallway mailboxes, where postman leave it. The data reachable on Sarajevogas website with this code include UIN, name, address and monthly debts of the customer (Krsman, 2009b).

4. In April 2010, the nongovernmental organization Kroacija Libertas filed with State Investigation and Protection Agency criminal charges against editor of the political magazine "60 Minutes", Bakir Hadziomerovic, and against other persons employed at Agency for ID documents (IDDEEA), due to violating the Law. The charges alleged that in the past year, journalists and editors in this political magazine of Federal television continuously published photos of people, information about time and place of birth, current residence, UIN and other information downloaded from the software of the IDDEEA, which is under the jurisdiction of the BiH Ministry of Civil Affairs. IDDEEA dismissed allegations that representatives of this institution provided Federal television journalists access to protected personal data of citizens. This Agency claim that all control mechanisms of data protection have been implemented and integrated into the system, according to European Commission's recommendation, so such leak of information is impossible. (Krivična prijava, 2010). This controversial case is still pending, with very serious charges of criminal and irresponsible behavior of journalists who provided strictly copyrighted and personal data to general public, while some of these data should have been preserved by the state of BiH and its institutions.

Conclusion

The importance of data privacy and the worldwide efforts in regulation of this area reflected in BiH as well, with considerable delay comparing with EU countries. Some of the factors for dramatic improvement of recent data privacy legislation are the same in BiH like in most other countries. First of all it is rapid expansion of the information technology and its usage in data management. Among key factors are also democratization processes which urge respect of human rights. Another factor is more regional, and it regards EU integration processes requiring legislation compliance. Finally, specific factor is environment based on ex political system legacy in BiH, which made these efforts challenging.

BiH has aspiration to go towards EU integration with fast pace, and on this road it is trying to enact all regulations with full compliance with EU standards. Thus, it completely integrated general principles of European data privacy into the Law on Personal Data Protection of BiH, with special respect to EU Directive requirements which became world standard on promoting data privacy protection.

Personal Data Protection Agency of BiH is working hard to implement these regulations, but the practice of personal data misuse transferred from old system is hard to eliminate. Recent cases illustrate inability of easy

implementation of data privacy protection, and its application is far from being satisfactory. Relevant independent international reports prove that additional efforts are needed for data privacy regulation functioning in practice.

To make a progress in data privacy protection, BiH need to raise awareness of data subjects, first of all citizens, who still don't hesitate to give in their personal data when inquiring certain benefits. Then it needs to raise awareness of public administration and public enterprises which are still among most serious violators. Public administration demonstrated its commitment to the unacceptable practice of being comfortable in collecting and having control over citizen's personal data. And lastly, BiH needs judicial system that will ensure efficient trial of data privacy violations, to eliminate practice of recent cases, where violators passed unpunished.

References

About the Agency. (2010). Personal Data Protection Agency of BiH. Retrieved May 8, 2010, from http://www.azlp.gov.ba/index.php?type=1&a=pages&id=1

Agencija zatražila izmjene Zakona o ličnoj karti [The agency has requested amendments to the Identity Card Law]. (2010, February 8). Retrieved May 8, 2010, from http://www.24sata.info/vijesti/dogadjaji/25860-Agencija-zatrazila-izmjene-Zakona-licnoj-karti-drzava-gradjanima-krade-licne-podatke.html

Bennett, C.J., & Raab, C.D. (1997). The adequacy of privacy: The European Union Data Protection Directive and the North American Response. Information Society, Jul-Sep97, Vol. 13, Issue 3.

Brown, D.H., & Blevins, J.L. (2002). The Safe-Harbor Agreement Between the United States and Europe: A Missed Opportunity to Balance the Interests of E-Commerce and Privacy Online. Journal of Broadcasting & Electronic Media, Dec2002, Vol. 46 Issue 4.

Council of Europe. (1950). Convention for the Protection of Human Rights and Fundamental Freedoms. Retrieved from http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=005&CL=ENG

Council of Europe. (1981). Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Retrieved from http://conventions.coe.int/Treaty/EN/Reports/HTML/108.htm

Council of Europe. (1987). Summary of the Committee of Ministers Recommendation No. R(87) 15 to the Member States on regulating the use of personal data in the police sector. Retrieved from http://polis.osce.org/library/details?doc_id=2670&_ru=%2Flibrary%2Fdetails%3Fdoc_id%3D2658

Council of Europe. (1995). Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal L 281 of 23.11.1995. Retrieved from http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf and http://europa.eu/legislation_summaries/information_society/l14012_en.htm

Directive on privacy and electronic communications. (2002, July 12). Directive 2002/58/EC of the European Parliament and of the Council of concerning the processing of personal data and the protection of privacy in the electronic communications sector. Official Journal L 201 of 31.07.2002. Retrieved from http://europa.eu/legislation_summaries/information_society/l24120_en.htm

E-Privacy Directive, The. (2003). Freshfields Bruckhaus Deringer, November 2003. Retrieved from http://www.freshfields.com/publications/pdfs/practices/7078.pdf

EU će budno pratiti poštivanje zaštite ličnih podataka [EU will closely monitor compliance with data protection]. (2010, March 23). Retrieved May 8, 2010, from http://www.nezavisne.com/dogadjaji/vijesti/55789/EU-ce-budno-pratiti-postivanje-zastite-licnih-podataka.html 23.03.2010

European Commission. (2009). Annex of the updated assessment of the implementation by Bosnia and Herzegovina of the roadmap for visa liberalisation. Retrieved from http://www.esiweb.org/rumeliobserver/wp-content/uploads/2009/07/detailed-conditions-for-bh.pdf

European Commission. (2010, April 19). Updated Assessment of the implementation by Bosnia and Herzegovina of the roadmap for visa liberalization. Retrieved from http://www.esiweb.org/pdf/White%20List%20Project%20Paper%20-%20Bosnia%20assessment%2019%20April%202010.pdf

European Court of Human Rights. (2007). Case of Copland v. United Kingdom. (2007) 45 EHRR 37, [2007] ECHR 253. Retrieved from http://www.bailii.org/eu/cases/ECHR/2007/253.html

European Union provided 250.000 euro for the project "Support to the Personal Data Protection Agency in BiH". (2009, October 14). Retrieved from http://www.delbih.ec.europa.eu/?akcija=vijesti&akcija2=pregled&jezik=2&ID=539

Federal Trade Commission. (2007). Fair Information Practice Principles. Retrieved from http://www.ftc.gov/reports/privacy3/fairinfo.shtm

General Assembly of the United Nations. (1948, December 10). The Universal Declaration of Human Rights. Retrieved from http://www.un.org/en/documents/udhr/

Gilbert, F. (2003). Privacy Laws - An Overview. IT Law Group. Retrieved from http://www.itlawgroup.com/Resources/Publications/PrivacyOverview.html

Herold, R. (2002). Overviews of Privacy-Related U.S. Laws and Regulations. The Privacy Papers: Managing Technology, Consumer, Employee, and Legislative Actions. Boca Raton, FL: CRC Press LLC.

Information Commissioner's Office. (1998). Data Protection Act. United Kingdom legislation. Retrieved from http://www.ico.gov.uk/what_we_cover/data_protection.aspx

Institucije BiH nezakonito traže uvjerenje o nekažnjavanju [Institutions of BiH illegally seeking a certificate of no criminal record]. (2009, December 19). Retrieved May 8, 2010, from http://www.radiosarajevo.ba/content/view/17128/63/

Interresorna radna grupa za pregovore o liberalizaciji viznog režima za građane Bosne i Hercegovine. (2009). Izvještaj o izvršavanju Plana aktivnosti za ispunjavanje preostalih obaveza iz Mape puta za liberalizaciju viznog režima za period 15.07.2009. – 07.09.2009. [Report on implementation of Action Plan for fulfilling the remaining commitments under the Roadmap for the liberalization of visa regime for the period 15.07.2009. – 07.09.2009]. Vijeće Ministara BiH, Sarajevo, 07.09.2009. p.31-32.

Kazagic, E. (2009, December 18). Zaštita ličnih podataka [Protection of Personal Data]. Retrieved from http://www.hayat.ba/vijesti/hayat-vijesti/14182-zatita-linih-podataka

Krivična prijava protiv Bakira Hadžiomerovića [Criminal charges against Bakir Hadziomerovic]. (2010, April 20). Retrieved May 8, 2010, from http://www.nezavisne.com/dogadjaji/vijesti/58256/Krivicna-prijava-protiv-Bakira-Hadziomerovica.html

Krsman, N. (2009a, December 22). Petar Kovačević: Lični podaci su svojina građanina, a ne države [Petar Kovacevic: Personal data is the property of the citizen, not a state]. Retrieved May 8, 2010, from http://www.nezavisne.com/dogadjaji/intervju/50803/Petar-Kovacevic-Licni-podaci-su-svojina-gradjanina-a-ne-drzave.html

Krsman, N. (2009b, February 06). Lični podaci dostupni u haustoru [Personal data available in the hallway]. Retrieved May 8, 2010, from http://www.nezavisne.com/dogadjaji/vijesti/36589/Licni-podaci-dostupni-u-haustoru.html

Law on Protection of Personal Data. (2006). Official Gazette of Bosnia and Herzegovina 49/06. Comments retrieved from http://www.esiweb.org/pdf/schengen_white_list_bosnian_visa_breakthrough.pdf p.52

Official Gazette of Bosnia and Herzegovina. (1999, 2004, 2009). No. 6/99, 7/04, 51/09, 52/09, 67/09 and 76/09.

Organization for Economic Co-operation and Development. (1980, September 23). Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Retrieved May 8, 2010, from http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html

Reding, V. (2010, January 28). Europeans' Privacy will be big challenge in next decade. European Commission's press release IP/10/63. Retrieved May 8, 2010, from http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/63

Robinson, N., Graux, H., Botterman, M., & Valeri, L. (2009). Review of the European Data Protection Directive. Information Commissioners Office (ICO), UK. Santa Monica, CA: RAND Corporation. Retrieved from http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/review_of_eu_dp_directive.pdf

Safe Harbor. (2000). US-EU Safe Harbor Framework. US Department of Commerce. Retrieved from http://www.export.gov/safeharbor/

Secretary's Advisory Committee on Automated Personal Data Systems. (1973, July). Records, Computers and the Rights of Citizens. Retrieved May 8, 2010, from http://aspe.hhs.gov/DATACNCL/1973privacy/tocprefacemembers.htm

Sjednica Vijeća Ministara. (2009, July 21). Održana 10. tematska sjednica Vijeća ministara BiH [10th thematic session of the Council of Ministers held]. Council of Ministers press release. Retrieved May 8, 2010, from http://www.vijeceministara.gov.ba/saopstenja/sjednice/saopstenja_sa_sjednica/?id=8782

Stabilization and Association Agreement between Bosnia and Herzegovina and the European Communities and their member states. (2008). Retrieved May 8, 2010, from http://www.dei.gov.ba/bih_i_eu/ssp/doc/Default.aspx?id=2952&pageIndex=1

Staples, W.G. (2007). Encyclopedia of privacy. Westport, CT: Greenwood Press.