DIGITAL RIGHTS NGO

Personal Data Protection Policy Guideline

Publication of this report is supported by Open Society Foundations - Armenia, grant N18773. The opinions and analyses expressed in the report are those of the authors and do not represent opinions and positions of Open Society Foundations – Armenia.

December 2014, Yerevan

Andranik Markosyan, Susanna Akritova

Contents

1. The purpose of policy guidelines

The main purpose of Personal Data Protection Policy Guidelines is to assist civil society activists and progressive policy makers in advocating relevant policy reforms. The Guidelines are composed of … parts each addressing specific personal data protection policy issue. First and second parts provide general guidelines. First part is focused on legislation and indicates relevant European standards that Armenia is committed to adopt with the ratification of the Council of of Europe Convention on Protection of Individuals with regard to Automatic Processing of Personal Data and Additional Protocol. Second part is devoted to enforcement issues and provide practical information about the national and international instruments and practices. Third part is aimed to provide information about the European practices related to institutional models of personal data supervising authorities, which is strongly depends on legal traditions and vary from country to country. And, finally, fourth part provides judicial practices of personal data enforcement that may help both civil society and legal professionals in defending individuals rights in regard to automatic protection of their personal data.

2. Legislation

Appropriate legislation is obviously the key element of data protection policy and must be shaped in a way to meet best international practices. The Council of Europe Convention on Protection of Individuals with regard to Automatic Processing of Personal Data is the most effective instrument for the harmonization of personal data protection legislation across the European countries. As a part of the European civilization and member of the Council of Europe Armenia need to adopt personal data protection policy in line with the European standards.

The main rationale of the adoption of sound data protection legislation is economic: appropriate protection of personal data is the basis for the development of knowledge based economy, which is the only chance of integration into the contemporary world economics. Meantime, appropriate level of personal data protection is required for the modernisation of public service, introduction of electronic governance tools, which in its turn reduces risks of corruption and abuse of administrative power. And last, but not the least reason is the respect of individuals privacy, which is fundamental right protected under fundamental human rights treaties

It would be correct to say that following the standards defined under the Council of Europe Convention will guarantee compliance with minimal requirements of both: rapidly growing information technologies market and e-government tools an important element of the modernisation of the society. These standards could be presented in five conceptual principles.

1. **Personal data must be obtained and processed fairly and lawfully. While the notion of lawfulness is widely used in Armenian legal system the concept of fairness is not that**

common and requires explanation. In the context of personal data protection it means that data controllers and data processors must obtain personal data honestly: either with consent of data subject or in strength compliance with the law. This also means that data controller/processor must not simply ensure formal compliance with laws and regulations, but also avoid any misuse of formal procedure that in spite of formal compliance are not in interest of data subject or purpose of relevant regulation.

2. **Personal data must be stored for specified and legitimate purposes and not used in a way incompatible with those purposes.** Principle of legitimate purpose and appropriate use of personal data is well known, always declared but according to the Human Rights Court practices is not always properly enforced even in traditional democracies. Even legitimately obtained data might be used for purposes other than it was collected. Even when doing so data controller thinks it act in good faith it violates this principle.

3. **Adequate, relevant and not excessive in relation to the purposes for which they are stored.** Even legitimately collected data should not be more than it is required for the purpose of its collection. However, this principle does not exclude a case of storing data for broader purpose if it prescribed under the law or agreed by data subject. However, general, broader purpose does not mean storage "just in case", but for a purpose of individuals or public interest, such as, for instance, general citizens register or telephone directory (white book). First case is a general purpose prescribed under the law, second is database created also created for the public purpose with consent of data subjects.

4. **Kept accurate and, where necessary, up to date.** The principle defines individuals subjective right to demand for accurate and up to date keeping of its information and the state's positive obligation to introduce relevant legal instruments. Positive obligation of state must be implemented in adoption of rules and regulation for the administration of public databases (regular update and accuracy measures), as well as, minimal requirements for privately stored data with special regimes for those of private databases that also has public importance (notaries, public utilities and other privately run services of public importance).

5. **Preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.** Fair use of data is a fundamental value of personal data processing policy. Destruction of data out of use is part of this approach and must be mandatory for both public and private database owners (data controllers). As mentioned, both law and data owner consent can define uncertain purpose such are maintenance of citizens register, criminal records or telephone directory.

3. Enforcement

Sanctions and remedies are the main mechanism of the enforcement of the personal data protection legislation. The Council of Europe Convention does not specify specific sanctions to be introduced by the signatory countries leaving these to legal traditions and public interest of member states. However, general approach in European countries is the following:

a) monetary, usually administrative sanctions are used in case negligence, unfair and/or non-proper collection, storage and processing, and

b) criminal fines and penalties for wilful and knowledgeable violations of individuals rights, usually if such a violations caused in material or moral damage.

It is worth to note that administrative sanctions are usually defined for specific violations rather than violations in general. In most of the European countries administrative sanctions are foreseen for non-fulfilment of notification duty, breach of data collection, storage, processing and distraction rules. Notably, legitimate destruction of data became an issue later, when value of computer stored data increased.

In Czech Republic fine for violation of data protection law by a natural person (individual) vary from $4,900 to $248,000 mln. depending on how serious is the offence. Legal entities could be penalized by a fine from $$248,000 to $496,000. Sanctions in Poland also strong and could be up to 50,000 Euro for breach of data protection law or decision of General Inspector on data protection. A person liable for willful violation of data protection law by a data controller (legal entity) could be fined from EUR 25 to EUR 270,000 or by imprisonment for the terms of up to three years. In Hungry penalties are not as high as in Czech Republic and Poland and vary from $460 to $4,600. Meantime, abuse of personal data could be punished by between one to three years by imprisonment depending on circumstances. Romanian law defines sanctions for non-notification or incomplete notifications (EUR 120 - EUR 2,235), illegal processing of personal data (EUR 230 - EUR 5,800), failure to provide certification on request of the authority (EUR 230 - EUR 3,500) and non-fulfilment of the security measures (EUR 3,500 - EUR 11,700).

French law provides vary of sanctions and remedies depending on the nature and circumstances of a violation. For instance, authority may issue an order to comply with the legislation in case of minor violations. In case of more serious violations data protection authority may impose a fine equal up to EUR 150,000 (for a first violation) or up to EUR 300,000 or 5% of the data controller's turnover (limited to EUR 300,000) (for a second violation). For wilful and knowledgeable violations French law stipulates stronger sanctions: up to five years imprisonment and/or a fine up to EUR 300,000 (for natural persons). A fine up to EUR1.5 million and/or other sanctions are stipulated for legal persons in case of major breaches of the law. Sanctions foreseen in other EU states are very similar to those in France.

Sanctions for data protection violation in post-soviet countries are not as strong as in EU members states. For instance in Russian Federation violation of data protection legislation (illegal collection,

storage and/or disclosure of personal data) is punishable under the Code of Administrative Violations by fine from $10 to $15 for individuals, from $15 to $30 for officials and from $150 to $300 for corporates. It is worthy to note that disclosure of personal data by either corporate or governmental officials is punished by a very minor fine, which is lower than sanctions for the breach of driving rules. In Ukraine sanctions for violation of data protection legislation have been introduced in 2012. Similar to Russian Federation sanctions are foreseen for both individuals and corporates and vary from $415 to $825. Criminal liability in Russia and Ukraine is stipulated only for illegal collection, storage and disclosure of confidential information of personal character (secrecy of private and family life). More detailed information on sanctions defined in some other EU member states and some non-EU countries is provided in Annex I.

To ensure proper level of enforcement Armenian legislative must have administrative and criminal liabilities. Monetary sanctions applicable to data controller for negligence, unfair and/or non-proper collection, storage and processing, and criminal fines and penalties might be imposed for wilful and knowledgeable violations of individuals' rights and usually if violations caused in material or moral damage. It is worth to note that administrative sanctions are usually defined for specific violations rather than violation of law in general, e.g. without specification of a particular article. In most of the European countries administrative sanctions are foreseen for non-fulfilment of notification duty, breach of data collection, storage, processing and distraction rules.

.

4. Institutional models of data protection authorities

Recommendations concerning the institutional and legal foundations ensuring effective operation of data protection authority is especially important due to the vary of data protection authority models applied across the Europe.. Preliminary review of data protection authorities of the European countries demonstrates variety of institutional schemes from fully institutionally independent authorities (Information Commissioner's Office of the United Kingdom) to a ministry based department with some elements of independent operations (State Data Protection Inspectorate in Lithuania). Taking into account the main principle of the project attention is paid on formal requirements of the Convention, which is in case of personal data protection supervisory authority is its independence.

Additional Protocol to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data defines the following requirements for the personal data protection authorities:

1. Supervisory authorities shall have, powers of investigation and intervention, as well as the power to engage in legal proceedings or bring to the attention of the competent judicial

authorities violations of provisions of domestic law giving effect to the principles mentioned in the Convention.

2. Supervisory authority shall hear claims lodged by any person concerning the protection of his/her rights and fundamental freedoms with regard to the processing of personal data within its competence.
3. Supervisory authority shall exercise their functions in complete independence.
4. Decisions of the supervisory authority, which give rise to complaints, may be appealed against through the courts.

It is worth to note that project environment has been change since the project beginning and apart from the analysis of acting Law on Personal Data the the project team also responded with comments to draft Law on Personal Data Protection and have to take into account these circumstances in recommendations on data protection authority. In other words recommendations on institutional models of data protection authorities are developed by the project team with assumption that the status and institution model proposed under the draft law is the most probable one and are focused on the improvement of the proposed model.

Proposed draft Law on Protection of Personal Data provides supervisory authority with substantial power of investigation and intervention, including, but not limited to issue of action order, suspension of data processing, blocking and distraction of data processed illegally (Article 23 of the Draft Law). Meantime, as an administrative body data protection authority will act in accordance with the Law on Basis of Administration and Administrative Proceedings and judicial enforcement could be the only instrument, which also means implementation of the requirement on judicial appeal. The Law on Basis of Administration and Administrative Proceedings also guarantees hearing complains of individuals who seeks enforcement of personal data protection legislation.

Independence of public authorities is the most complicated and often controversial issue that lawmakers face when adopting personal data protection legislation. When speaking about independence of public authority institutional experts usually means ability of the authority to act independently, e.g. not be exposed to a pressure from political leadership (presidency, cabinet, parliamentary majority) of the country. Independance of a public authority from political leadership is usually achieved through transparent appointment mechanisms, limited power of political leaders over the dismissal of an independent authority, financial independance of an authority enabling its operation without a financial support from government or presidency.

The review of European practices in institutional models of data protection authorities is primarily focused on study of abovementioned elements of independance in the view of Armenia data protection authority model proposed under the currently discussed draft Law on Personal Data Protection.

Appointment of data protection authority (head of institution and/or member)

Baltic states are a bright example of rapid and effective transformation of a post-soviet country into a progressive EU member state with effective government and experience of Baltic states is very important also due to the similar scale of human and financial resources. In Latvia Data State Inspectorate is managed by a director who is appointed and released from his or her position by the Cabinet of Ministers pursuant to the recommendation of the Minister for Justice. Similarly, Lithuanian data protection authority, the Data Protection Inspectorate, is managed by the Director who recruited for a term of office of five years and dismissed by the Government in accordance with the procedure established by the Law on the Government. Head of Estonian data protection authority, the Data Protection Inspectorate is also appointed by the government for the terms of five years. Candidacy of the head of Inspectorate is proposed by the Ministry of Internal Affairs.

Estonian law provides detailed circumstances of the dismissal of the head of Inspectorate guaranteeing independence of the authority:

1. at his or her own request;
2. due to expiry of term of office;
3. for a disciplinary offence;
4. due to long-term incapacity for work;
5. upon the entry into force of a judgment of conviction with regard to him or her;
6. if facts become evident which according to law preclude the appointment of the person as a director general.

It is worth to mention that draft Law on Protection of Data Protection proposed by the Armenian government provides pretty same mechanisms of appointment and dismissal, with the sole exception of status of the authority that supposed to be within the ministry of justice, which, by the way, is acceptable model prescribed under Latvian and Lithuanian laws. Meantime, the experience of Estonia is prefered due to higher status and emphasis of the independance.

Netherlands is one of EU states that managed to build effective data protection system. Personal data protection authority in Netherlan, the Data Protection Commission, composed from a chairperson and two members. The chairperson is appointed by a Royal decree on proposal of prime minister for a terms of six years. Two other members appointed through similar procedure for the terms of four years. Additionally, the Commission has an advisory board to advise the Commission on general aspects of the protection of personal data. The members shall be drawn from the various sectors of society and shall be appointed by Our Minister, on the proposal of the Commission.

Financial independance

Latvian data protection law missing funding provision and Lithuanian simply refer to state budget funding. Estonian law also does not provide guarantees of the financial independance of Data Protection Inspectorate and even Netherlands Personal Data Protection Act, which describes all the procedures, responsibilities of subjects to regulation in details does not contain funding provisions.

Public accountability

What is really missing in both acting and prospective data protection legislation of the Republic of Armenia is the concept of accountability of personal data protection authority.

Latvian legislation requires data protection authority tp produce and publish annual report on its activities, but does not provide any detailed requirements towards the format and/or a feedback (parliamentary or in form of hearings). Estonian law requires Data Protection Inspectorate to public report on inspections carried out and the results, as well as presentation of annual report to Constitutional Committee of the Estonian parliament. The report of Estonian Data Protection Inspectorate should provide an overview of the most important facts related to the compliance and application of the Data Protection Act during the preceding calendar year. Dutch data protection authority report to the Cabinet of Ministers and publishes it on the web site. The report of Dutch Data Protection Commission must cover “the activities, policy pursued in general and the effectiveness and efficiency of its mode of operation in particular during the preceding calendar year”.

It is worthy to note that accountability is not just an instrument for civil control over the public authorities, but also element of their independence: a public authorities reporting to legislative and making report to public is more independent than those report to ministers cabinet or presidency.

Today policy issues and guidelines

Advisory body composed of representatives of non-governmental human/civil rights organizations with experience not less than 10 years, would be an effective instrument granting the authority public trust and professional experience. However, the law shall contain mechanisms guaranteeing appointment of a person with real experience respected by majority of human / civil rights defending NGOs.

Financial independence of data protection authority is better to defined under the law to exclude possible pressure and influence of government. Such a guarantee could be a provision stating that budget of the authority per staff member shall not be less than per one staff member budget of ombudsmen office. Best practice of the financial independence is provided in the law on Public Utilities Regulation Commission, though it depends on regulatory payments that could not be a case in area of personal data protection. However, linking budget to a particular, stable public institutions (for instance remuneration paid to members of parliament) would be ideal mechanism of financial independance.

For the efficiency of the operation of data protection authority a concept of public accountability should be introduced in form of annual report to National Assembly and official publication. Additionally, if created, an advisory board could produce opinion on the report/activities of the authority.

5. Judicial practices

Understanding of cases of the European Court of Human Rights is important for developing relevant practices of judgments under the national legislation. It is worthy to note, that European Court of Human Rights rulings are based on the European Human Rights Conventions and protection of personal data is considered by the Court from that perspective and most of the personal data protection cases are considered as an implication of Article 8 of the Convention.

Case of the Court of Justice of the European Union could not be considered as a reference case law in Armenia, but might be useful in terms of understanding of European standards. It especially truth for cases related to challenging the independence of national personal data protection authorities by the European Commission. Independence of regulatory authorities in Armenia was always a subject of criticism from civil society and international organizations. One of the main obstacles of the independence of regulatory authorities are career perceptions of their members and absence of independent funding mechanisms. Relevant case of the Court of Justice of the European Union might demonstrate CJEU approaches towards the concept of public authorities independence.

One of a bright cases of the personal data protection violation is the Shimovolos v. Russia case. This case demonstrates how the European Court of Human Rights handles the cases related to the protection of personal data in respect of individuals rights to be aware about the personal data collected and stored, as well as, lawfulness of data collection. The applicant's name has been registered in surveillance database with reference "human rights activist" among skinheads and other categories of individuals that according to the interior services (police) are involved in

extremist activities. On the way of traveling to 2007 EU-Russia Summit in Samara the applicant has been stopped several times for identity check and after series of checks he was brought to police station with formal reasons as “committing administrative offence”.

The Court ruled that private life is a broad term not susceptible to exhaustive definition. Article 8 of the Convention is not limited to the protection of an “inner circle” in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. It also protects the right to establish and develop relationships with other human beings and the outside world. Private life may even include activities of a professional or business nature.

Representative of the Russian mainly referred to the exceptions defined under the Article 8 of the Convention, e.g. intervention of public authorities in private life of citizens “in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.” Court ruled that collection of data was not in accordance with the law and was not necessary for protection of public order and security.

Having regard to its case law the Court found that the collection and storing of that data amounted to an interference with his private life as protected by Article 8 § 1 of the Convention. The Court also founds in this case violation of Article 2 of the Protocol 4 granting individuals freedom of movement within the territory of a state and also violation of Articles 5 and Article 14 of the Convention (right to liberty and security and prohibition of discrimination).

Another interesting case is Ciubotaru v. Moldova, which is typical for administrative proceedings in post-soviet countries. The applicant, Mihai Ciubotaru, applied to the Moldovan authorities to change his old Soviet identity card by a Moldovan identity card. On the application form he wrote “Romanian” under ethnicity. However, he was told that his application would not be accepted unless Moldovan ethnicity was indicated on it. The applicant complained and later was informed that since his parents were not recorded as ethnic Romanians in their birth and marriage certificates, it was impossible for him to be recorded as an ethnic Romanian. He was advised to search the National Archives for traces of Romanian origin of his grandparents and other ancestors.

The applicant wrote numerous complaints to the Prime Minister, the President of the country and other officials, but to no avail. The applicant tried to challenge the decisions at judicial institutions, but without any success: on 6 April 2005 the Supreme Court of Justice dismissed the applicant's appeal on points of law and pointed out that according to section 68 of the Law on Documents

pertaining to Civil Status (see paragraph 16 below) it was impossible to change his parents' ethnic identity to Romanian because in none of their identity papers had Romanian ethnicity been indicated.

Moldavian government submitted that Article 8 of the Convention was not applicable in the present case because the right to respect for private life did not cover the right to ethnic identity and that there was no interference with the applicant's rights under that provision.Moldavian government also argued that a blanket acceptance of requests concerning changes in ethnic identity, based solely on the applicants' declaration but not on evidence, could lead to serious consequences of an administrative nature, referring thus to paragraph 2 of the Article 8 of the Convention. The Government suggested that the applicant's desire to be recorded as an ethnic Romanian might be motivated by his intention to obtain Romanian citizenship and argued that it was within the Government's margin of appreciation to determine the extent to which requests concerning changes in records concerning ethnic origin could be accepted.

The Court reiterated that the concept of “private life” is a broad term not susceptible to exhaustive definition. It covers the physical and psychological integrity of a person. The Court also stated that the notion of personal autonomy is an important principle underlying the interpretation of the guarantees provided for by Article 8. Under this principle protection is given to the personal sphere of each individual, including the right to establish details of their identity as individual human beings. The Court also stated that along with such aspects as name, gender, religion and sexual orientation, an individual's ethnic identity constitutes an essential aspect of his or her private life and identity.

The Court noted that consideration of ethnic identity as a privacy life is particularly true in the current social setting of the Republic of Moldova, where the problem of ethnic identity has been the subject matter of social tension and heated debate for a long time and, more importantly, where an individual's recorded ethnic identity, unlike other recorded aspects of identity, is decisive for the determination of the ethnic identity of his or her children and of the next generations. Accordingly, the facts of the present case fall within the ambit of “private life” under Article 8 of the Convention and since the authorities refused to record the applicant's declared ethnic identity, he may claim to be a victim of a breach of the provisions of this Article. The Court therefore dismisses the Government's preliminary objection regarding non-applicability of the Article 8 of the Convention.

The Court specifically considered efforts that Moldavia authorities (including judicial) undertook for prove of ethnical identity of the applicant, i.e. language, name, empathy and others. However, his request concerning the change of recorded ethnicity was refused on sole ground of missing records proving the applicant's ethnical identity. The Court found that the State failed to examine the applicant’s claim to belong to a certain ethnic group in the light of the objectively verifiable evidence adduced in support of that claim. The Court therefore concluded that the authorities failed to

comply with their positive obligation to secure to the applicant the effective respect for his private life. There has, accordingly, been a breach of Article 8 of the Convention.

In case Cemalettin Canlı v. Turkey relates to unlawful disclosure of personal data by law enforcement bodies in respect of pending criminal proceedings. In 1990 the applicant was prosecuted for his alleged membership of an illegal organisation, namely Dev-Genç ("Revolutionary Youth") but was acquitted on 25 September 1990. Another set of criminal proceedings brought against him under Article 141 of the Criminal Code for membership of another illegal organisation, namely Dev-Yol ("Revolutionary Path"), were discontinued in 1990 following the repeal of that provision. On 23 August 2003 the applicant was on his way to a demonstration in Ankara, organised by the Confederation of Public Workers' Unions. He was arrested by the police, who allegedly beat him up. He was taken to a police station. A police report drawn up the same day stated that the applicant had a previous record for terrorist related activity in 1990.

On 24 August 2003 the Ankara prosecutor filed an indictment, accusing the applicant and 25 other persons of contravening the Demonstrations Act, and charged them with the offences of damaging State property and resisting arrest by using force. While the criminal proceedings were pending before the Ankara Criminal Court of First Instance (hereinafter "the Ankara court"), a police report entitled "information form on additional offences" was submitted to the Ankara court. In the report, under the heading "Records of Guilt", were two entries stating that the applicant was a member of Revolutionary Youth organization. The report, which also included the applicant's fingerprints, address and birth registry details, had been drawn up in accordance with Article 12 of the Police Regulations on Fingerprinting, which empowered the police to keep such details on persons accused or convicted of certain offences.

The applicant complained to the prosecutor with reference to the fact of the termination of criminal prosecution for membership of Revolutionary Path and drawing the prosecutor's attention to the fact that Police Regulations on Fingerprinting also required the police to include in their records any acquittals or discontinuations of criminal proceedings. He asked the prosecutor to prosecute the police officers who had neglected their duties by failing to comply with the Regulations. However, the prosecutor dismissed the applicant's request for the police officers to be prosecuted. The prosecutor considered that the officers had not attempted to mislead anyone; all they had done was to forward to a criminal court official records of past incidents concerning the applicant. The applicant lodged an objection against the prosecutor's decision and argued that the prosecutor had not examined or even mentioned in his decision the Regulations in question before deciding not to prosecute the police officers. He further complained that his rights under the European Convention on Human Rights, in particular his rights to a fair trial and to respect for his private and family life, had been breached. The applicant's objection was rejected by the Sincan Assize Court on 17 March 2004.

The applicant complained that the records kept arbitrarily and unlawfully by the police and the publication in the national press of the details of those records had had adverse effects on his private life within the meaning of Article 8 of the Convention. The Government argued that the complaint was inadmissible on account of the applicant's failure to exhaust domestic remedies. According to the Government, the applicant could have asked the administrative courts to rectify the records. However, the applicant had failed to bring this complaint, even in substance, to the attention of the domestic authorities. The Government further argued that the applicant had failed to bring an action against the newspapers which published the details of the police report. In the opinion of the Government, the complaint filed with the prosecutor was irrelevant in so far as it aimed to seek redress for the keeping of the records, because the keeping of the records had a legal basis; the complaint filed with the prosecutor could have been an effective remedy only if an offence had been committed.

The applicant submitted that he had been unaware of the records until they were submitted to the Ankara court in 2003 and, as such, it was illogical to expect him to have applied to the relevant authorities to amend those records prior to 2003. After they had been submitted to the court in Ankara in 2003 it was too late, as he had already been portrayed in the media as a member of terrorist organisations. According to the Court's established case-law, where an applicant has a choice of domestic remedies, it is sufficient for the purposes of the rule of exhaustion of domestic remedies that that applicant makes use of the remedy which is not unreasonable and which is capable of providing redress for the substance of his or her Convention complaints. Once the applicant has used such a remedy, he or she cannot also be required to have tried others that were also available but probably no more likely to be successful.

In the instant case, the Court observes that, according to Article 230 of the Criminal Code of Turkey in force at the time of the events, it was an offence for a public servant to delay in carrying out or to omit to carry out his or her duties. Moreover, Article 26 of the Police Regulations on Fingerprinting sets out in an unambiguous fashion the circumstances in which police records are to be amended to include information on acquittals or discontinuations relating to the criminal charges mentioned in those records. Indeed, it is not disputed by the Government that it was the duty of police officers to amend their records. The Court considers that it was reasonable for the applicant to conclude that the police officers had committed the offence defined in Article 230 of the Criminal Code by failing to perform their duties, and to make an official complaint to the prosecutor. It is also to be noted that, contrary to what was submitted by the Government, in the course of his submissions to the prosecutor and the Assize Court the applicant expressly referred to his rights under the Convention.

Resuming the case the Court found that the drafting and submission to the Ankara court by the police of the report in question was not “in accordance with the law”, within the meaning of Article 8 § 2 of the Convention. This conclusion makes it unnecessary to examine whether the other requirements of paragraph 2 of Article 8 were complied with. The Court considered that the applicant must have suffered non-pecuniary damage, such as distress and frustration, on account of the publication in the press of defamatory information about him, which cannot be sufficiently compensated by the finding of a violation alone. Making an assessment on an equitable basis, it awarded the applicant EUR 5,000 under this head and EUR 1,500 as a compensation for the proceedings before the Court.

Case of K.U. v. Finland (applicant requested not to disclose his name is interesting in the light of expansion of digital technologies and electronic communication network. On 15 March 1999 an unidentified person or persons placed an advertisement on an Internet dating site in the name of the applicant, who was 12 years old at the time, without his knowledge. The advertisement mentioned his age and year of birth, gave a detailed description of his physical characteristics, a link to the web page he had at the time, which showed his picture, as well as his telephone number, which was accurate save for one digit. The applicant became aware of the advertisement on the Internet when he received an e-mail from a man, offering to meet him.

The applicant’s father requested the police to identify the person who had placed the advertisement in order to bring charges against that person. The service provider, however, refused to divulge the identity of the holder of the so-called dynamic Internet Protocol (IP) address in question, regarding itself bound by the confidentiality of telecommunications as defined by law. The police then asked the Helsinki District Court to oblige the service provider to divulge the said information pursuant to section 28 of the Criminal Investigations Act. In a decision issued on 19 January 2001, the District Court refused since there was no explicit legal provision authorising it to order the service provider to disclose telecommunications identification data in breach of professional secrecy. The court noted that by virtue of Chapter 5a, section 3, of the Coercive Measures Act and section 18 of the Protection of Privacy and Data Security in Telecommunications Act the police had the right to obtain telecommunications identification data in cases concerning certain offences, notwithstanding the obligation to observe secrecy. However, malicious misrepresentation was not such an offence.

The applicant submitted that Finnish legislation at the time protected the criminal, whereas the victim had no means to obtain redress or protection against a breach of privacy. Under the Penal Code the impugned act was punishable, but the Government had neglected to ensure that the Protection of Privacy and Data Security in Telecommunications Act and the Coercive Measures Act were consistent with each other. He argued that the random possibility of seeking civil damages, particularly from a third party, was not sufficient to protect his rights. He emphasised that he did not have the means to identify the person who had placed the advertisement on the Internet. While

compensation might in some cases be an effective remedy, this depended on whether it was paid by the person who had infringed the victim's rights, which was not the case in his application. According to the Government, new legislation was in place which, had it existed at the time of the events, would have rendered this complaint unnecessary.

The Government emphasised that in the present case the interference with the applicant's private life had been committed by another individual. The impugned act was considered in domestic law as an act of malicious misrepresentation and would have been punishable as such, which had a deterrent effect. An investigation had been initiated to identify the person who had placed the advertisement on the Internet, but had proved unsuccessful due to the legislation in force at the time, which aimed to protect freedom of expression and the right to anonymous expression. However, most essential in this case was that even the legislation in force at the material time provided the applicant with means of action against the distribution of messages invading his privacy, in that the operator of the Internet server on which the message was published was obliged by law to verify that the person in question had consented to the processing of sensitive information concerning him or her on the operator's server. This obligation was bolstered by criminal liability and liability in damages. Thus, the legislation provided the applicant with sufficient protection of privacy and effective legal remedies.

In its ruling the Court noted at the outset that the applicant, a minor of 12 years at the time, was the subject of an advertisement of a sexual nature on an Internet dating site. The identity of the person who had placed the advertisement could not, however, be obtained from the Internet service provider due to the legislation in place at the time. Although this case is seen in domestic law terms as one of malicious misrepresentation, the Court would prefer to highlight these particular aspects of the notion of private life, having regard to the potential threat to the applicant's physical and mental welfare brought about by the impugned situation and to his vulnerability in view of his young age. The Court reiterated that, although the object of Article 8 is essentially to protect the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private or family life. These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves. The Court stated that there are different ways of ensuring respect for private life and the nature of the State's obligation will depend on the particular aspect of private life that is at issue.

As to the Government's argument that the applicant had the possibility to obtain damages from a third party, namely the service provider, the Court considered that it was not sufficient in the circumstances of this case. It is plain that both the public interest and the protection of the interests of victims of crimes committed against their physical or psychological well-being require the availability of a remedy enabling the actual offender to be identified and brought to justice, in the

instant case the person who placed the advertisement in the applicant's name, and the victim to obtain financial reparation from him. The Court found that there has been a violation of Article 8 of the Convention in the present case.

Apparently, cases of national courts and European Court of Justice are very different in ground, though quite similar in nature. Unlike EHRC, which is mainly judge taking into account its own cases the European courts proceed cases on the basis of national legislation and EU legislation including, but not limited to fundamental EU documents (EU Charter and Community agreements) Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive), Directive 95/46/EC on the protection of individuals with regard to the processing

of personal data and on the free movement of such data (Data Protection Directive). The cases described below demonstrates judicial practices of national courts of the European Union and judgment of the European Court of Justice.

Telecommunications is one of the industry there personal data protection is always raise disputes due to the growing technical means where users data stored by the undertakings and users themselves. On of such cases is Kärntner Landesregierung and Others the Austrian Constitutional Court submitted questions to the CJEU concerning the validity of Articles 3 to 9 of Directive 2006/24/EC (Data Retention Directive) in light of Articles 7, 9 and 11 of the Charter and whether or not certain provisions of the Austrian Federal Law on Telecommunications transposing the Data Retention Directive were incompatible with aspects of the Data Protection Directive and of the EU Institutions Data Protection Regulation.

Mr Seitlinger, one of the applicants in the Constitutional Court's proceedings, held that he uses the telephone, the internet and email both for work purposes and in his private life. Consequently, the information which he sends and receives passes over public telecommunication networks. Under the Austrian Telecommunications Act of 2003, his telecommunications provider is legally required to collect and store data about his use of the network. Mr Seitlinger realised that this collection and storage of his personal data was in no way necessary for the technical purposes of getting the information from A to B on the network.

Nor, indeed, was the collection and storage of these data even remotely necessary for billing purposes. Mr Seitlinger had certainly not consented to this use of his personal data. The sole reason for the collection and storage of all of these extra data was the Austrian Telecommunications Act of 2003. Mr Seitlinger, therefore, brought an action before the Austrian Constitutional Court in which he alleged that the statutory obligations on his telecommunications provider were breaching his fundamental rights under Article 8 of the EU Charter.

Case of the European Court of Justice are quite different from those of ECHR. For example, such case as European Commission v. Germany,197 the European Commission had requested the CJEU to declare that Germany had incorrectly transposed the requirement of 'complete independence' of the supervisory authorities responsible for ensuring data protection and thus failed to fulfil its obligations under Article 28 (1) of Data Protection Directive. In the Commission's view, the prob- lem was that Germany had put under State oversight the authorities responsi- ble for monitoring the processing of personal data outside the public sector in the different federal states (Länder). The assessment of the substance of the action depended, according to the Court, on the scope of the requirement of independence contained in that provision and, therefore, on its interpretation.

The Court underlined that the words "with complete independence" in Article 28 (1) of the directive must be interpreted based on the actual wording of that provision and on the aims and scheme of the Data Protection Directive. The Court stressed that the supervisory authorities are "the guardians" of rights related to personal data processing ensured in the directive and that their establishment in Member States is thus considered "as an essential component of the Court concluded that "when carrying out their duties, the supervisory authorities must act objectively and impartially. For that purpose, they must remain free from any external influence, including the direct or indirect influence of the State or the Länder, and not of the influence only of the supervised bodies".

The CJEU also found that the meaning of 'complete independence' should be interpreted in light of the independence of the EDPS as defined in the EU Institutions Data Protection Regulation. As underlined by the Court, Article 44 (2) thereof clarifies the concept of independence by adding that, in the performance of its duties, the EDPS may neither seek nor take instructions from anybody. This rules out state supervision of an independent data protection supervisory authority.201. Accordingly, the CJEU held that the German data protection institutions at federal state level responsible for monitoring the processing of personal data by non-public bodies were not sufficiently independent because they were subject to oversight by the state.

Another case of challenging the independance of personal data protection authority has been brought by the European Commission to the European Court of Justice against Austria. In the European Commission v. Austria the CJEU highlighted similar problems concerning the position of certain members and the staff of the Austrian Data Protection Authority (Data Protection Commission, DSK). The Court concluded in this case that Austrian legislation precluded the Austrian Data Protection Authority from exercising its functions with complete independence within the meaning of the Data Protection Directive. The independence of the Austrian DPA was not sufficiently assured, because the Federal Chancellery supplies the DSK with its workforce, oversees the DSK and has the right to be informed at all times about its work.

ANNEX I

Sanctions and remedies for the violation of data protection legislation in different jurisdictions

Jurisdiction	Sanctions available for data breaches
Austria	The penalty for the illegal access to a computer system is a fine or up to six months' imprisonment. Administrative penalties of up to EUR 25,000 apply for: Willful illegal data access. Willful illegal data transfer. Illegal processing, despite a binding court ruling. Willful deletion of data, despite a request for information. Administrative penalties of up to EUR 10,000 apply for cases in which: The duty of notification is violated. Data is transmitted to a recipient outside Austria without the permission of the DSK. A data controller does not comply with its duties to inform the data subjects or the DSK. If the necessary security measures have not been taken. An administrative penalty of up to EUR 500 applies for cases in which the data subject's right of information, the right to correction and deletion, or the right of objection (*see Question 13*) is infringed and the violation is not subject to one of the aforementioned higher penalties.
Australia	The Office of the Australian Information Commissioner can issue determinations including declarations that: The respondent has engaged in conduct constituting interference with the privacy of an individual and must

	not repeat or continue such conduct. The respondent must perform any reasonable act or course of conduct to redress any loss or damage suffered by the complainant. The complainant is entitled to a specified amount by way of compensation for any loss or damage.
Austria	Imprisonment of up to one year for a wilful infringement of data protection legislation with the intention of unjustified enrichment or to harm another person. Administrative penalties of up to EUR25,000 for certain breaches of data protection legislation. In some cases of data protection infringement, the Penal Code (*Strafgesetzbuch*) may apply, providing for financial fines or imprisonment.
Belgium	The processing of personal data in breach of the DPL may constitute a criminal offence, penalised with fines up to EUR550,000. Any repeat offences are punishable by a term of imprisonment from three months to two years, and/or a fine of EUR550 to EUR550,000.
Brazil	Collective damages order resulting from a class action. No limit on the amount of damages. Administrative fine of up to about US$1.7 million, if consumer rights are involved.
Canada	The sanctions for violations of privacy legislation differ based on the jurisdiction within Canada and the specific offence. The highest legislative sanction available for failure to maintain adequate security safeguards for an organisation is Can$100,000. Compliance orders, orders to publish corrective notices

	and orders for damages are also possible.
China	According to the Rules for the Protection of Personal Information of Telecommunication and Internet Users, if the internet and telecom service providers commit violation of the provision regarding the data protection, the telecom regulator may impose administrative fines ranging from RMB10,000 to RMB30,000 and warn them to rectify. The service providers in question may also be subject to criminal prosecution.
Czech Republic	Non-compliance with the PPD Act: Natural persons: less serious offences: up to CZK100,000; more serious offences: up to CZK1 million; more serious offence under certain circumstances: up to CZK5 million. Legal entities: general offences: up to CZK5 million; offences under certain circumstances: up to CZK10 million. Non-compliance with other regulations: Up to CZK1 million. In cases involving disclosure to the public: up to CZK5 million.
Finland	Personal data offence: fine or imprisonment up to one year. Personal data violation: fine. Computer break-in: fine or imprisonment up to one year. Aggravated computer break-in: fine or imprisonment up to two years. Secrecy offence: fine or imprisonment up to one year. Secrecy violation: fine. Breach and negligent breach of official secrecy: fine or imprisonment up to two years.

France	Under the general administrative sanctions regime, the CNIL can: Impose a fine up to EUR150,000 (for a first violation) or up to EUR300,000 or 5% of the data controller's turnover (limited to EUR300,000) (for a second violation). Order the data controller to immediately cease the data processing. Criminal penalties apply for certain offences, for example: Up to five years' imprisonment, and/or a fine up to EUR300,000 (for natural persons). A fine up to EUR1.5 million and/or other sanctions (for legal persons).
Germany	A maximum EUR300,000 fine for administrative offences. Criminal sanctions (maximum of to two years imprisonment or a fine). Reputation damages. Confiscation of profit and benefit derived from a violation. Civil liability and injunctive relief (under competition law).
Hungary	The Authority can impose a fine of between HUF100,000 to HUF1 million on the data controller. Abuse of personal data can be punished by between one to three years' imprisonment depending on the circumstances.
Ireland	Under Section 31 of the DPA: Maximum fine on summary conviction is EUR3,000. Maximum fine on indictment is EUR100,000. Under S.I. No. 336 of 2011: On summary conviction each call or message can

	attract a maximum fine of EUR5,000. If convicted on indictment the fines can be: a maximum of EUR50,000 for natural persons; a maximum of EUR250,000 for body corporates. It is necessary for the ODPC to apply to a court to impose these fines.
India	The remedies available for breach of data protection laws vary depending on the nature of the contravention. The penalty for non-compliance with the provisions of the IT RSPPSPI Rules is INR25,000 (*section 45, IT Act*). Penalties under the IT Act can extend up to INR50 million and include imprisonment. Specific penalties include the following, among others: Tampering with computer source documents (*section 65, IT Act*): imprisonment up to three years and/or a fine of up to INR200,000. Offences as provided in section 43 of the IT Act (*section 66, IT Act*): imprisonment up to three years and/or a fine of up to INR500,000.
Italy	Depending on circumstances, data breaches can attract sanctions of: Fines of up to EUR1.2 million. Imprisonment of up to three years.
Japan	Failure to file a report of a security breach or filing a false report when requested by a governmental ministry can result in a maximum fine of JPY300,000. Failure to take recommended measures to correct data protection security breaches can result in an order to take those measures. Violating an order can lead to fines up to JPY300,000 and imprisonment (with labour) of up to six months.

Luxembourg	Criminal fines for breaches to the data protection rules can range from EUR251 to EUR125,000 or imprisonment from eight days up to one year, or both. The data protection authority can also impose various administrative sanctions.
Mexico	The main sanctions for non-compliance are economic fines, though criminal offences are also included in the Personal Data Protection Law.
Norway	The Data Inspectorate can: Issue fines of a maximum of 10 times the National Insurance Basic Amount, currently EUR110,000. Order the cessation of unlawful processing. Impose conditions which must be met to bring the processing in compliance with the PDA. Impose coercive fines which will run for each day from expiry of the time limit set for compliance until the order has been complied with. More serious breaches (wilful or grossly negligent) can result in sanctions from the prosecuting authorities (fines and imprisonment, in severe circumstances, for a maximum of three years). The controller may also be liable to compensate the data subject for both financial and non-financial damages.
Poland	Liability under the PDPA. Failure to comply with decisions of the General Inspector may result in a maximum fine of about EUR50,000. Criminal liability. A person who is liable (usually a member of a management board of the company which is the data controller) may be subject to: a fine (from about EUR25 to EUR270,000); a partial restriction of freedom; a prison sentence of up to three years.
Qatar	There is no specific data protection law. Various laws provide

	for certain privacy rights and protections, the breach of which may give rise to a criminal offence (and subsequently penalties of imprisonment and/or a fine) and/or civil remedies.
Qatar (including Qatar Financial Centre (QFC))	The QFCA can make recommendations to data controllers, issue them with warnings or admonishments, and bring breaches to the attention of the QFC Regulatory Tribunal. The QFCA does not impose fines and instead has a policy of assisting firms to prevent non-compliance.
Romania	The level of fines range from about: EUR120 to EUR2,325 for failure to file the notification or filing an incomplete or bad-faith notification. EUR230 to EUR5,800 for illegal data processing operations to include those made by processors. EUR230 to 3,500 for failure to provide the authority with the required clarifications. EUR3,500 to EUR11,700 for failure to comply with the security measures.
Russian Federation	A maximum administrative fine of RUB10,000. Orders to cure violations. Criminal liability (with a maximum sentence of two years). Suspension of the violating company's business activity.
Saudi Arabia	SAR5 million or five years' imprisonment or both (for breaches of the Electronic Transactions Law). Fines beginning from SAR5 million for breaches of the Telecommunications Act and Anti-Cyber Crime Law 2007. A maximum fine of SAR3 million and four years' imprisonment apply to breaches of personal data privacy laws.

	Additional sanctions may apply under *sharia* law.
South Africa	Protection of Personal Information Bill: administrative fine of up to ZAR10 million for certain offences under the PPI Bill (which is not yet in force). Consumer Protection Act: administrative fines of up to 10% of a respondent's turnover or ZAR1 million for offences with regard to provisions contained in the CPA relating to direct marketing.
Spain	Depending on the severity of the breach, fines from EUR40,001 to EUR600,000. A cessation order, for very serious breaches (such as illegal use or transfer of data, which seriously affects the rights of data subjects). If this order is not complied with, the AEPD may freeze the relevant files. There are no criminal sanctions available.
Sweden	Default fines: Are rarely used in relation to the PDA and there is no established practice. Damages: Compensation to data subjects for non-pecuniary damages (normally EUR 120 to EUR3500) and the damage caused. Fines: The fines applied by Swedish courts rarely exceed EUR5,000. Imprisonment: Maximum six months respectively, in case of gross negligence or intent, maximum two years. Imprisonment sentences are very rare and the few imprisonment sentences rendered by Swedish courts have involved additional offences such as defamation.
Thailand	There are currently no sanctions or remedies for non-compliance with data protection laws. There are sanctions for Specific Businesses who must ensure appropriate security for data or face either: Between six and 18 months' imprisonment.

	A fine of between THB5,000 and THB20,000. Both of the above.
Turkey	Under the Criminal Code: Persons who store personal data unlawfully are subject to imprisonment from six months to three years. Persons who transfer or publish personal data unlawfully are subject to imprisonment of one to four years. Other fines and sanctions will apply under the Draft Law on Data Protection when in force.
United Kingdom	Fines up to GB£500,000 for serious breaches of the Data Protection Act or the Privacy and Electronic Communications (EC Directive) Regulations 2003. Enforcement notices requiring organisations to take (or refrain from taking) specified steps. Information notices requiring organisations to provide the ICO with specified information. Undertakings committing an organisation to a particular course of action. Assessment notices to conduct compulsory audits to assess an organisation's compliance. Prosecution for criminal offences under the DPA.
United Arab Emirates	There is no specific data protection law. However, various laws provide for certain privacy rights, the breach of which can give rise to criminal penalties (including imprisonment and/or fines) and/or civil remedies.
United Arab Emirates, Dubai International Financial Centre (DIFC)	Providing false or misleading information to the Commissioner: US$20,000. Non-compliance with a direction or order from the Commissioner: US$15,000. Processing sensitive personal data without the required permit: US$10,000. Transferring personal data outside the DIFC without

	the required permit: US$20,000.
USA	A consumer's actual damages and attorney's fees; and injunctive relief.