Open Society Foundations - Armenia

POLICY ANALYSIS

PRIVACY PROTECTION REMEDIES

The issue of personal data protection remedies is one of the key provisions (Art. 10) of the Council of Europe Convention on Protection of individuals with regard to Automatic Processing of Personal Data. It is important to note that Article 10 of the Convention specifically stresses necessity of "appropriate sanction and measures", e.g. existence of any measure cannot be viewed as fulfillment of the Convention requirements, but only if such measures are sufficient for the protection of individual's privacy.

Traditionally, remedies and sanction are discussed in the context of administrative and judicial enforcement. However, today many societies adopted quasi-judicial or quasi-administrative mechanisms such as, for example, office ombudsmen or appeal boards. However, administrative proceedings of data protection authorities remain the main mechanisms of data protection due to relatively short time of proceedings and ability to secure complaints, e.g. the issue of orders to protect individuals during the entire proceeding on case.

Non-Judicial Bodies

The powers of non-judicial bodies to address data protection violations vary across the European countries. Often people can seek remedy via an ombudsman, such as in the Czech Republic, Italy and the Netherlands. In the Czech Republic, the ombudsman (the Public Defender of Rights) is entitled only to ask the Data Protection Authority (DPA) to rectify a mistake. In Italy, the ombudsman for administrative acts of municipal, provincial and regional authorities can order that access to data be denied, either temporarily or permanently.

A number of bodies are also able to issue fines for data protection violations, for instance the Portuguese Communications Authority and the Italian Commission for access to administrative documents at the Office of the Prime Ministers, the Hungarian National Media and Information Communications Authority and the Austrian Administrative Authorities. A superior authority in Latvia can demand a public or written apology, as well as order compensation in the form of both pecuniary and nonpecuniary damages.

There is a variety of administrative sanctions available across the EU member states, including issuing an order a warning or objection, making different orders (e.g. to disclose information, to implement specific measures, to rectify, to erase or block specific data, to discontinue processing operation or suspend the transfer of data to a third state), imposing fines (pecuniary sanctions), revoking licenses or reporting the matter to courts or a public prosecutor.

Data Protection Authorities (DPA)

Data protection authorities often act as the first point of contact for victims of such violations, so they play an important role in remedying data protection violations. This role is often recognized by national courts, and in Finland, for instance, the prosecutors and courts are obliged to provide DPA with an opportunity to be heard in cases under the Finnish Personal Data Act.

The extent to which these tools are utilized varies across the EU Member States. European Union's Fundamental Rights Agency (FRA) data indicate that about half of the Member States empower DPAs to issue warnings or formal objections to the practices of controllers. In some Member States, allowing for the size differences between countries, these were used sparingly between 2009 and 2011; for example, in Luxembourg

one warning was issued, and in Cyprus eight were issued. In Romania and Slovenia, 66 and 158 warnings respectively were issued between 2009 and 2011[1].

The most common course of action taken by DPAs is issuing a fine or pecuniary sanction, as reported in 19 EU Member States. For example, the DPA in Cyprus issued fines in 20 cases between 2009 and 2011. During the same time period, the Spain's DPA issued 1715 fines, Czech Republic's DPA issued 279 fines, Estonia's issued 101, Latvia's 63, Romania's 148, Slovakia's 45, Sweden's two and the United Kingdom's nine. The size of the fine imposed is often set out in domestic legislation, and many EU Member States distinguish between natural persons (or individuals) and legal entities (or corporate bodies).

Fines can often be increased to punish when numerous violations have been committed. At the lower end of the scale, the DPA in Romania can issue fines up to €12,000, and the DPA in Slovenia can issue fines up to €830 for individuals and €12,510 for legal entities. Fines issued by the DPA in Hungary range from €350 to €35,000, and in Greece they range from €880 to €150,000 based on the severity of the violation. In Slovakia, fines can reach €332,000. In France, the DPA can issue fines of up to €150,000 for first violations, and up to €300,000 if a further violation is committed within five years.

At the upper end of the scale, the DPAs of the United Kingdom and Spain can issue fines of up to €500,000 and €600,000 respectively. In Poland, overall fines for not complying with a decision of DPA range from approximately €12,000 (a single-person business) to approximately €48,000 (company). A further punitive measure employed by DPAs in several EU Member States is revoking – either temporarily or permanently – licenses necessary for the processing of data. FRA data indicate that DPAs can revoke licenses or authorization to process data, but there are few recorded instances of this ability being used: six in Croatia between 2009 and 2011, and just one during the same period in Luxembourg. In sufficiently serious cases, some DPAs can refer the case to either the courts or the public prosecutor of the relevant EU Member State.

Judicial Procedures

With regard to civil and administrative procedures, most of the EU Member States explicitly recognise the ability to award compensation in the form of damages. Several Member States report that non-pecuniary compensation can also be granted. Whereas some Member States set out in domestic legislation the amount of compensation that can be awarded, often it is left to judges to develop an accepted range of both pecuniary and non-pecuniary damages through national case law. Again, the amounts awarded vary greatly between Member States.

In serious enough cases, criminal proceedings can be initiated for violations of data protection legislation. As the research demonstrates, there are a number of possible outcomes once court proceedings have been initiated: the courts can issue warnings; publicize any judgment made; prohibit an individual from managing the processing of data in the future; and compel those responsible for the violation to undertake community service. In addition, in all EU Member States the courts can impose fines, issue a prison sentences or combine both. The size of the fine or length of the prison sentence is set out in national legislation and varies between the Member States. Much like the civil and administrative procedures in place, the sentence will be affected by whether the violation involves natural persons or legal entities.

For those imprisoned, the majority of EU Member States enforce a maximum determinate sentence, most of which fall between six months (Croatia and Malta) and five years (Cyprus, France, Slovenia and Latvia). Within this range fall Belgium (two years), Estonia (one year), Finland (one year), Germany (two years), Hungary (three years), Luxembourg (one year), Poland (three years), Portugal (four years), Slovakia (three years) and Sweden (two years). In Denmark, a sentence of up to four months can be imposed. In Greece, the Court of First Instance can issue a sentence of up to three years, with the Court of Appeal may increase this to 10 years. In

[1] Very reports of the European Union Agency for Fundamental RIghts.

Spain, the maximum sentence is seven years' imprisonment, whereas in Romania no upper limit is imposed on judges. In Ireland and the United Kingdom, no custodial sentence is applied for data protection violations.

Intermediaries (Civil Society and other informal institutions)

Civil society organisations play a role in providing advice, guiding and taking complaints, providing a valuable addition to the statutory data protection framework. The fieldwork targeted intermediaries – representatives of the civil society organisations or other individual professionals that provide support for the individuals subject to the data protection violations and aimed to capture the opinions and experiences of those who help complainants navigate justice systems in seeking remedies in the data protection area.

The representatives of different organisations covered by the fieldwork play an important role in bridging gaps when individuals access justice in the complex area of data protection. The intermediaries consider that the role civil society plays in providing advice, guiding and taking complaints is a valuable addition to the statutory data protection framework.

Other activities of the civil society organisations mentioned by research respondents included education, research and training. Other examples include targeted assistance to migrants in detention centres, when procedural issues have a data protection component. Civil society organisations and other intermediaries raise awareness and publicise issues through media campaigns, article and publications. They monitor the situation and focus on lobbying and campaigning.

Most Frequent Areas of Violation of Individual's Privacy

The individuals subjected to the data protection violations were asked about the violations that led them to seek redress. The results from the fieldwork covered a wide and diverse range of types and areas of the data protection violations faced by the research participants in the last three years before the research in all the 16 EU Member States. The most frequent data protection violations that were mentioned related to Internet-based activities. These included social media, online shopping, leakage of personal data from e-shops, hacking of email accounts and databases, identity theft, security breaches and misuse of personal data by global internet companies[2].

Internet-based activities clearly emerged as a high-risk territory for data protection. For example, one Finnish judge remarked that it is good that there is a special unit of police that has the ability to investigate computer crimes very thoroughly if there is need to do so. The 2011 Special Eurobarometer survey indicated that 43% of Internet users said they had been asked for more personal information than necessary when attempting to access or use an online service. The 2012 Special Eurobarometer survey on cyber security showed that, when using the Internet for online banking or shopping, Europeans had two main concerns such as someone taking or misusing personal data (mentioned by 40% of Internet users in the EU) and security of online payments (38%). Also, security concerns influenced the behaviour of internet users, as 37% of the survey respondents said they were less likely to give personal information on websites[3].

Another common data violation was direct marketing and commercial prospecting without the consent of the recipient, when the personal data were misused on mobile phones, by email or by post. The fieldwork suggests that mobile operators and debt collectors are often responsible for these violations. Irregular practices such as selling personal data to third parties were noted. The interviewees often referred to video surveillance (in particular, no signs warning about the surveillance) at the workplace, in the public spaces or in supermarkets.

[2] European Commission (2011). The survey was conducted in the EU27 between the end of November and mid-December 2010. A total of 26,574 Europeans aged 15 and over were interviewed. All interviews were conducted face to face in people's homes and in the appropriate national languages

[3] European Commission (2012d). The survey was conducted in the EU27 in March 2012. A total of 26,593 Europeans aged 15 and over were interviewed. All interviews were conducted face to face in people's homes and in the appropriate national languages.

Several individuals in different countries had also experienced secret surveillance conducted by public authorities with special technology or by secretly installed CCTV.

Most of the violations recorded in European countries are related to the processing of personal data, such as collection, storage, disclosure and dissemination, for example:[4]

- Unjustified transfer of personal data from data controllers (employers, public authorities, mobile operators, credit institutions, etc.) to third parties. In this context, it is worth mentioning the unauthorised transfer of data to debt collection companies by credit institutions and selling databases with contact details of persons by commercial companies.
- Storage of inaccurate or unnecessary information.
- Manipulation of inaccurate personal data stored and processed legally.
- Unlawful disclosure of personal data to unauthorised persons.
- Unlawful disclosure by the justice system of confidential personal data related to domestic violence during a criminal case and divorce proceedings.
- Publication of personal data in the media or on Internet.
- Publication of personal data of parties in proceedings in the legal databases or on the Intranet in courts' databases.

The other data protection violations are connected to the rights of the data subject, especially with his or her right of access:

- refusals of access to personal data held by the police, medical services, social services, employers and others or insufficient responses to requests for access to personal data;
- refusals to correct, delete and block information in personal data files (such as law enforcement, health sector) or insufficient responses to requests for corrections, deletion and blocking of information in personal data files.
-

Public authorities (national and local governments, and law enforcement authorities) and private entities (e.g. media companies and financial institutions alike) were alleged to have violated data protection.

Proposed actions

- Mapping potential privacy protection risks in Armenia and development of relevant recommendation for DPA.
- Deeper study of European countries experience of sanctions and remedies: both, legal framework and enforcement practices, assessment of relevant practices in Armenia and development of recommendations for DPA and legislative on improvement of legal framework and practice.
- Comparative study of the European and Armenian judicial practice and development of recommendations for Armenian educating judicial on enforcement of national legislation in the context of ECHR case law.

Author: **Andranik Markosyan**
Digital rights expert
Email: andranik@gmail.com
November 2016

Publication of this policy analysis is supported by Open Society Foundations - Armenia. The opinions and analyses expressed in the paper are those of the author and do not necessarily represent opinions and positions of Open Society Foundations – Armenia.

[4] European Centre for Disease Prevention and Control (ECDC) (2013).