Second Study Commission Questionnaire 2010

ESTONIA

Civil Issues Regarding the Protection of Privacy (with Particular Focus on Such Matters as Affected by the Internet)

A. Laws and regulations

1) What laws apply to protection of privacy issues in your legal system? Are there civil code/legislative/common law provisions that protect individuals against violations regarding:

a) In the public sector

- Access by individuals to information collected by various government agencies about them?
- Protection from disclosure of that information to third parties?
- Access by the media or members of the public to government records, for example, those regarding government decision-making and action, and limitations put on that access?
- Limitations put on information sharing between government agencies?

The main laws regulating the above-mentioned fields in Estonia are **Personal Data Protection Act** (hereinafter mentioned as PDPA) and **Public Information Act** (hereinafter mentioned as PIA).

**The aim of PDPA** is to protect the fundamental rights and freedoms of natural persons upon processing of personal data, above all the right to inviolability of private life. The Act protects the fundamental rights and freedoms of persons with respect to the processing of their personal data and in accordance with the right of individuals to obtain freely any information that is disseminated for public use. Since 2008 personal data is divided into two categories, namely "personal data" and “sensitive personal data” as the sub-class under special protection. For clarity purposes, the definition of “personal data” has been specified in the draft Act, stating that the protection of personal data shall extend to all forms of data, including audio and graphic data as well as biometric data. Data protection is supervised by the Data Protection Inspectorate.

**The purpose of PIA** is to ensure that the public and every person has the opportunity to access information intended for public use, based on the principles of a democratic and social rule of law and an open society, and to create opportunities for the public to monitor the performance of public duties. This act also includes provisions establishing databases

As a conclusion, one can say that everybody has a right to access to information collected about them by public bodies. Upon processing of personal data, a processor of personal data is required to adhere to the principle of individual participation - the data subject shall be notified of data collected concerning him or her, the data subject shall be granted access to the data concerning him or her and the data subject has the right to demand the correction of inaccurate or misleading data. The collected information must be protected from the access of third parties unless otherwise foreseen by law.
Access by the media or members of the public to government records and other public documents has been provided by PIA. In order to ensure democracy, to enable public interest to be met and to enable all persons to exercise their rights and freedoms and perform their obligations, holders of information are required to ensure access to the information in their possession under the conditions and pursuant to the procedure provided by law. Access to information shall be ensured for every person in the quickest and easiest manner possible. Upon granting access to information, the inviolability of the private life of persons shall be ensured. Every person has the right to contest a restriction on access to information if such restriction violates the rights or freedoms of the person.

The Chancellery of the Parliament, the Office of the President of the Republic, the Office of the Chancellor of Justice, the State Audit Office, courts, government agencies and legal persons in public law are also required to maintain web sites for the disclosure of information.

Limitations of the access may arise from law. First of all, some information is considered as state secret and therefore not disclosed.

Some data are to be classified as information intended for internal use only, for example information collected in criminal or misdemeanour proceedings (except for the information subject to disclosure under the conditions provided by the Code of Misdemeanour Procedure and the Code of Criminal Procedure), information collected in the course of state supervision proceedings until the entry into force of a decision made thereon, information the disclosure of which would damage the foreign relations of the state etc.

The head of a state or local government agency or a legal person in public law may classify some data as information intended for internal use, e.g. draft legislation of general application before it is sent for approval or presented for passage, draft documents and accompanying documents before receipt or signature thereof, in justified cases, documents addressed to persons within the agency which are not registered in the document register (opinions, notices, memoranda, certificates, advice, etc.) information which may damage the interests of the state acting as a participant in the proceedings in a civil proceeding, until the court decision is made).

In cases, named in law, a holder of information who is a state or local government agency may not classify data as information intended for internal use and thereby set access restrictions. Such cases are e.g. results of public opinion polls, generalised statistical surveys, economic and social forecasts, notices concerning the state of the environment, reports on the work or the work-related success of the holder of information and information on the quality of the performance of duties and on managerial errors as well as the information which damages the reputation of a state or local government official, etc.

Restrictions of privacy

Some restrictions arise from Surveillance Act that foresees the conditions and procedure for surveillance in order to guarantee the security of persons and to detect and combat criminal offences.

Security Authorities Act foresees some restrictions on right to confidentiality of messages, right to inviolability of home or private and family life. The justification of such restrictions arises only from the objective of security authorities that is to ensure the national security and constitutional order by non-military means of prevention and to collect and process information necessary for formulating the security policy and for the national defence. The law foresees special procedure for such actions. There is also a special Security Authorities Surveillance Committee of the Parliament which exercises supervision over agencies of executive power in questions relating to the activities of security authorities and surveillance.
agencies, including assurance of fundamental rights and efficiency of the work of security authorities and surveillance agencies, and in questions relating to supervision exercised thereover.

In some areas there are special legal acts regulating additionally privacy protection and access conditions in the respective area (for example, Health Services Organisation Act foresees special regulations as regards obtaining information from Health Information System).

If a person finds that his/her rights have somehow been violated, he/she can either apply to the superior body or agency of the violating administrative organ and apply for supervisory control, or apply to Data Protection Inspectorate or court.

b) In the Private Sector

- Protection from disclosure to third parties of personal information collected in the world of e-commerce, for example
  - personal information provided through the use of credit/debit cards and other electronic transfers of funds;
  - personal information in relation to credit reporting and banking transactions;
  - records of a customer’s usage (telephone; online activity);
  - records kept for insurance coverage and other social services benefits provided by the private sector?

- Protection from surreptitious collection of information via the internet, for example, through internet electronic surveillance technologies such as “spyware” or “adware”?

First of all, the main legal act, PDPA is also applicable in the private sector.

The general law that regulates the protection of personal information in the private sector is also Law of Obligations Act (hereinafter referred to as: LOA). According to LOA the unjustified use of the name or image of the person, breaching the inviolability of the private life or another personality right of the person is considered unlawful unless otherwise provided by law. Upon the establishment of unlawfulness, the type of violation, the reason and motive for the violation and the gravity of the violation relative to the aim pursued thereby shall be taken into consideration. The violation of a personality right is considered not to be unlawful if the violation is justified considering other legal rights protected by law and the rights of third parties or public interests. In such case, unlawfulness shall be established based on the comparative assessment of different legal rights and interests protected by law.

Some special laws foresee more rules. For example, Credit Institutions Act foresees that all data and assessments which are known to a credit institution concerning of the clients of the credit institution or other credit institutions are deemed to be information subject to banking secrecy. Details of a client which are subject to banking secrecy may be disclosed by a credit institution to third persons only with the written consent of the client, unless the obligation or right to disclose information subject to banking secrecy arises from the provisions of law (for example if such an information shall be demanded by a court or pre-trial investigation authority or the Prosecutor's Office if a criminal proceeding is commenced). The managers and employees of a credit institution and other persons who have access to information subject to banking secrecy are required to process the data in conformity to the Personal Data Protection Act and maintain the confidentiality of such information indefinitely, unless
otherwise provided for in law. Similar obligations arise for Insurance Companies and Investment Funds from Insurance Activities Act and Investment Funds Act respectively.

There are also several legal acts that regulate the conditions of rendering services through internet or providing services of electronic communication. For example, Estonia has adopted Information Society Services Act (hereinafter mentioned as ISSA) in order to fulfil the requirements of E-commerce Directive (2000/31/EC). ISSA provides for the requirements for information society service providers, the organisation of supervision and liability for violation of this Act. “Information society services” are considered to be all such services provided in the form of economic or professional activities at the direct request of a recipient of the services, without the parties being simultaneously present at the same location, and such services involve the processing, storage or transmission of information by electronic means intended for the digital processing and storage of data. Information society services must be entirely transmitted, conveyed and received by electronic means of communication.

There is also Electronic Communications Act, in order to create the necessary conditions for the development of electronic communication to promote the development of electronic communications networks and communications services without giving preference to specific technologies and to ensure the protection of the interests of users of electronic communications services by promoting free competition and the purposeful and just planning, allocation and use of radio frequencies and numbering.

One must also mention that The Estonian Information Society Strategy 2013 was approved by the Order of the Government of the Republic Nr 667 (of 30 November 2006). It is a sectoral development plan, setting out the general framework, objectives and respective action fields for the broad employment of ICT in the development of knowledge-based economy and society in Estonia in 2007-2013. Several international and EU-level policy documents, notably the EU i2010 and eGovernment action plans, were taken into consideration when elaborating the strategy. The document also includes notes about privacy issues to be taken account when implementing this strategy. Relevant legislation, including privacy, consumer protection and information security related aspects, will be reviewed.

As a member of Council of Europe Estonia is also bound by the practice of European Court of Human Rights; the issues of privacy mainly arising from the conflict of articles 10 and 8 of the European Convention on Human Rights (right to freedom of expression, right to hold opinions and to receive and impart information versus the protection of private life, family, correspondence etc).

2) What laws apply with respect to the investigation and enforcement of privacy rights?
   - How strong is the protection?
   - Are the laws binding or advisory?
   - How does an individual make a complaint when a private actor or government breaks privacy laws?
   - Who prosecutes or enforces – for example, a privacy commissioner, administrative body, such as a privacy tribunal?
   - Is there a right to a court remedy?
   - Are there out-of-court dispute resolution options?
The enforcement of privacy rights can take place either through court or through Data Protection Inspectorate. The person, whose right is or has been violated by unlawful processing of personal data, does not have to apply to the Data Protection Inspectorate or to some other institution before he/she can apply to court.

Data Protection Inspectorate has a right to conduct proceedings, in case person's rights have been violated in matters of unlawful processing of personal data. Data Protection Inspectorate is the extra-judicial body which also conducts proceedings in matters of misdemeanours provided for in law.

The Data Protection Inspectorate may also issue a precept which requires a holder of information to bring its activities into accordance with law if the Inspectorate finds, for example, that the holder of information has refused illegally to comply with a request for information or has failed to disclose information subject to disclosure as required.

According to LOA, if unlawful damage is caused continually or a threat is made that unlawful damage will be caused, the victim or the person who is threatened has the right to demand that behaviour which causes damage be terminated or the making of threats with such behaviour be refrained from. In the case of violation of inviolability of personal life or any other personality rights, it may be demanded, *inter alia*, that the tortfeasor be prohibited to approach other persons (restraining order), the use of housing or communication be regulated or other similar measures be applied. For example, court can issue an order and to prohibit the tortfeasor to approach or contact the victim via all means of communication.

In case damage occurs, the victim has a right to demand compensation according to the general principles – any person (tortfeasor) who unlawfully causes damage to another person (victim) shall be obliged to compensate for the damage if the tortfeasor is culpable of causing the damage or is liable for causing the damage pursuant to law.

If the rights of a data subject have been violated upon processing of personal data, the data subject has the right to demand the compensation of the damage caused to him or her:

1) on the basis and pursuant to the procedure provided by the *State Liability Act* if the rights were violated in the process of performance of a public duty, or
2) on the basis and pursuant to the procedure provided by the LOA if the rights were violated in a private law relationship.

Procedural aspects of investigating and processing complaints as well as solving disputes are respectively regulated in Code of Civil Procedure, Code of Administrative Procedure, PIA and PDPA.

Laws, regulating the enforcement of privacy rights are mostly binding. The Data Protection Inspectorate has also elaborated a set of instructions in several fields of data protection. Such instructions are considered to be recommendations for data processors suggesting how private data should be processed. The above-mentioned instructions are advisory.

**B. Private-Sector Initiatives**

1) Do particular companies, industries or professional associations in your country govern themselves regarding the protection of privacy? For example, are there privacy policies, professional codes, voluntary industry standards?

2) Who or what body, if any, ensures that these standards are met?
There is such a self-governing system for journalists. Estonian Newspaper Association is a non-profit organisation working in the common interests of newspapers. It unites 40 newspapers published in Estonia. One of the aims of this organisation is also in conjunction with Press Council to uphold good journalistic practice. It has produced The Code of Ethics of the Estonian Press that includes several provisions as regards journalism standards that are also connected to privacy protection. For example, art 3.7. of the Code states, that a journalist shall use honest means of obtaining audio or video recordings and information, with the exception of cases where the public has a right to know information that cannot be obtained in an honest way. Art 4.6.-4.8. state that information and speculation about an individual’s mental or physical health shall not be disseminated unless the individual is willing or the information is in the public interest. As a rule, child custody battles should not be covered. When covering crime, court cases and accidents, the journalist shall consider whether the identification of the parties involved is necessary and what suffering it may cause to them. Victims and juvenile offenders shall not be identified as a general rule.

The body, that ensures that these standards are met, is a voluntary self-regulatory Press Council (Pressinõukogu). The Press Council was set up by the Estonian Newspaper Association and is active since 2002.

The Press Council and internet news portals have also signed an agreement under which the Press Council will handle complaints regarding the journalistic content of these sites. News portals, which are not attached to traditional newspapers, agree to conform to the Estonian code of press ethics and undertake the obligation to honour the Press Council's rulings on them.

If a person reckons his/her rights (incl privacy) have been violated by a journalist, he/she can apply to the Press Council and the latter will take a position as regards the violation and make a ruling.

There are some more professional codes of ethics for specific professions that foresee confidentiality obligations. Such provisions usually are complementary to legal regulations which means that the same obligations actually arise from law as well. For example, Code of Conduct of the Estonian Bar foresees confidentiality obligations for attorneys as regards their clients. An attorney shall accordingly respect the confidentiality of all information given to him by his client or received by him about his client or others in the course of rendering services to his client. An attorney shall ensure that no third person had access to his client’s documents, correspondence or other information, or to any documents drafted by the advocate which are in his possession in connection with handling the client’s matter. The obligation of confidentiality is not limited in time. The attorney shall comply with the confidentiality obligation also after the termination of his professional activities.

Violations of such requirements shall be discussed and solved either in the Court of Honour of the Bar that has been set up by the Bar Association or in court.

C. International and Cross Border Issues

1) How is privacy protected when information is exchanged or transferred to other countries?

2) Are there any agreements, laws or international treaties or protocols, to protect privacy issues in this situation?

3) Does your country limit its exchange of information to countries with similar protections of privacy?
The main principle for the transmission of personal data to foreign countries is stipulated in PDPA. According to law, the transmission of personal data from Estonia is usually permitted only to a country which has a sufficient level of data protection.

Transmission of personal data is permitted to the Member States of the European Union and the States party to the Agreement of the European Economic Area, and to countries whose level of data protection has been evaluated as sufficient by the European Commission. Transmission of personal data is usually not permitted to a country whose level of data protection has been evaluated as insufficient by the European Commission. Personal data may be transmitted to a foreign country which does not meet the conditions only if the data subject has granted permission to this or with the permission of the Data Protection Inspectorate if the chief processor guarantees, for that specific event, the protection of the rights and inviolability of the private life of the data subject in such country and the sufficient level of data protection is guaranteed in such country for that specific case of data transmission. The Data Protection Inspectorate shall inform the European Commission of the grant of such permission.

It must also be mentioned, that Estonia has ratified the Convention for the Protection of Individuals with regard to processing personal data.