

IMPLEMENTATION OF THE EU LEGAL FRAMEWORK FOR DATA PROTECTION, WITH SPECIFIC REFERENCE TO THE LAW ON PERSONAL DATA PROTECTION OF THE REPUBLIC OF MACEDONIA

March 2006

One of the pre-conditions for development of the Information Society is for users (individuals, commercial enterprises and governmental bodies) to have confidence or “trust” in the reliability, security, and integrity of electronic communications systems and computerized information processing systems. One crucial component of the trust framework is privacy protection.

Information privacy or data protection is based on a set of principles for collection, exchange and use of personal data in commercial and governmental contexts. Data protection laws permit, and even facilitate, the commercial and governmental use of personal data while at the same time providing to individuals (1) control over what to disclose; (2) awareness of how their personal data will be used; (3) rights to insist that data are accurate and up-to-date; and (4) access to data about themselves.

In 1995, the European Union adopted its Data Protection Directive (95/46/EC), establishing a detailed privacy regulatory structure for adoption into national law by EU member states.¹ In 2005, the Republic of Macedonia adopted a Law on Personal Data Protection, modeled on the EU Directive.

The Macedonian Law, like the EU Directive, reflects ten basic principles:

1. **Purpose Specification.** Personal data shall be collected only for purposes that are concrete, clear and legally determined. The subsequent use of data should be limited to those purposes. Article 5, paragraph 1, item 2.
2. **Notice.** The data subject shall be informed of the identity of the data controller and the purpose for which data are collected, as well as the rights of access and correction. Article 10. If data are not collected from the data subject, the controller shall at the time of recording of the data, inform the data subject of the controller’s identity, the purposes for which the data will be processed, the third parties to whom the data will be disclosed, and the right of the data subject to oppose such use or disclosure. Article 11.
3. **Collection Limitation.** Personal data should be collected only if it is appropriate, relevant and not excessive in relation to the purpose for which

¹ The EU Directive and many related resources are available at http://europe.eu.int/comm/justice_home/fsj/privacy/index_en.htm.

- it is collected (no more data should be collected than is necessary to accomplish the stated purpose). Article 5, paragraph 1, item 3.
4. **Data Quality.** Data should be accurate, complete, and up to date, taking into account the purposes for which they were collected. Article 5, paragraph 1, item 4. Upon request of the data subject, and upon its own initiative, the data controller is obliged to supplement, amend, or delete incorrect, incomplete or out-of-date information. Article 14.
 5. **Retention Limit.** Data should be stored in a form that allows identification of the data subject for no longer than is necessary to fulfill the purposes for which the data were collected. Article 5, paragraph 1, item 5.
 6. **Use Limitation.** Data should not be disclosed or processed except for purposes specified when it was collected unless the data subject consents, subject to specified exceptions. Article 6.
 7. **Access.** The data subject has the right to access data about himself. Article 12. This right is crucial to exercise of the right to data quality.
 8. **Security.** Any person having access to a personal data collection on behalf of a controller or handler of the collection is obliged to maintain the secrecy and protection of the data. Article 23. In order to ensure secrecy and protection of personal data, the controller must apply adequate technical and organization measures. Article 24.
 9. **Openness.** A data controller shall keep records of each personal data collection indicating its practices regarding that data collection and shall submit those records to the Data Protection Directorate, which shall compile and publish them. Articles 27-30.
 10. **Accountability and Enforcement.** The data “controller” should be accountable for complying with the protections and a process is created for data subjects to enforce their rights under the law. Articles 18-22; Articles 37-47 (creation and competencies of the Directorate); Articles 49-50 (penal provisions)

The Macedonian law has certain additional features, including special rules on the processing of the unique birth registration number of the citizen (Article 9) and a requirement that special categories of personal data may be transmitted through a telecommunications network only if encrypted (Article 8, paragraph 4).

The EU Directive and National Laws Based on It Can Be Implemented in a Flexible Fashion, to Avoid Undue Burdens on Data Controllers and Data Processors.

The EU Data Protection Directive, if read and enforced literally, is very broad and potentially very onerous. However, all EU regulation is based on the principle of “proportionality,” which means that regulations must be proportionate to the risk of harm and must take into account the national state of development. A regulatory agency should avoid actions that impose barriers to economic growth. Government regulatory power should be exercised only as necessary, proportional to the both the nature of the privacy harm and its likelihood. In addition, EU law grants Member States a “margin of manoeuvre” in implementing any of its Directives, allowing nations to develop somewhat different approaches depending on national circumstances.

The Data Protection Directive in particular includes provisions allowing flexible enforcement. For example, Article 18 of the Directive allows data controllers to avoid the notice requirements if they appoint a personal data protection officer (sometimes called a chief privacy officer) who maintains a notice of the data collected by the entity and how it is used.

In addition, the EU Data Protection Directive specifically encourages use of private sector “codes of conduct” “self-regulatory” measures, which can make the impact of the directive less burdensome. Industry codes of conduct allow regulation to be flexible, in order to keep pace with technological developments and with evolving industry practices. Codes can help avoid unnecessary regulatory barriers and can limit the arbitrary exercise of regulatory authority. (Self-regulation, of course, can never override express legislative requirements.) If industry sectors are still in developmental stages within the country, a new data protection authority may wish to make reference to codes of conduct developed by industry groups in the EU and otherwise to seek technical assistance from industry groups in the EU.

Additional Resources

In 2002, the EU adopted a second privacy directive, specifically addressing privacy in electronic communications services. Among other issues, the 2002 Directive on Privacy and Electronic Communications addresses unsolicited email and the use of personal information by communications companies. The 2002 Directive is available at http://europa.eu.int/comm/justice_home/fsj/privacy/law/index_en.htm.

GIPI Analysis of the 2002 EU Directive (October 2002)
<http://www.internetpolicy.net/privacy/privacy-memo.pdf>.

Resources on EU data protection law - overview, model contracts, links to other international instruments and national data protection commissioners
http://europa.eu.int/comm/justice_home/fsj/privacy/index_en.htm

The International Chamber of Commerce has developed a Privacy Toolkit for Policy Makers, http://www.iccwbo.org/home/e_business/word_documents/TOOLKIT-rev.pdf.

Center for Democracy and Technology, "Privacy and E-Government" (May 2003) - report to the United Nations Department of Economic and Social Affairs as background for the World Public Sector Report on E-Government. Surveys privacy trends internationally with a focus on data in the hands of government. Describes "best practices," including privacy officers, privacy impact assessments, privacy enhancing technologies and privacy audits.
<http://www.internetpolicy.net/privacy/20030523cdt.pdf>

For further information, contact Jim Dempsey, GIPI Policy Director, jdempsey@cdt.org