Executive summary of the public audit report

PROTECTION OF AUTOMATICALLY PROCESSED PERSONAL DATA

11 December 2013 No. VA-P-90-3-21

Full audit report in Lithuanian is available on the website of the National Audit Office: www.vkontrole.lt

DEFINITIONS AND ABBREVIATIONS

Definitions:

Personal data means any information relating to a natural person (data subject) who is known or who can be identified directly or indirectly by reference to such data as a personal identification number or one or more factors specific to their physical, physiological, mental, economic, cultural, or social identity.

Personal identification code means a unique sequence of eleven decimal digits intended for the identification of a natural person.

Data subject means a natural person who can be identified directly or indirectly by reference to a certain element of personal data (personal identification code, fingerprints, etc.) or a set of such elements (e.g. name, surname, date of birth, residence address). A person becomes a data subject from birth until death.

Rights of the data subject means the opportunities of data subjects to participate in and to control the activities of the data controller when processing their personal data.

Data processing means any operation carried out with personal data: collection, recording, accumulation, storage, classification, grouping, connecting, changing (supplementation or correction), provision, publication, logical and/or arithmetical operations, search, destruction, or any other action or set of actions. The list of data processing operations is not exhaustive, these operations may be performed both by the data controller and the data processor, as well as any other persons.

Data processing by automatic means is any operation performed with personal data carried out in whole or in part by automatic means. Such means are any kind of information and communication technology which enables its users to carry out personal data processing operations, for example, computers, communication networks, etc.

Data processor means a legal or a natural person other than an employee of the data controller, processing personal data on behalf of the data controller. The data processor may not take independent decisions concerning personal data processing – they must strictly abide by the instructions of the data controller.

Data controller means a legal or a natural person which alone or jointly with others determines the purposes and means of processing personal data. The data controller decides for what purpose and what personal data will be processed, who it will (or will not) be provided to, how the data subject's rights will be guaranteed, what organisational and technical measures for data security are, what hardware and software will be used to process the data, etc.

Special categories of personal data means data concerning racial or ethnic origin of a natural person, his political opinions or religious, philosophical or other beliefs, membership in trade unions, and his health, sexual life, and criminal convictions. In scientific literature, special categories of personal data are sometimes called sensitive data.

Abbreviations:

SDPI / Inspectorate means State Data Protection Inspectorate.

EXECUTIVE SUMMARY

Lithuania began to address the issues of personal data protection in 1992 when the Constitution was adopted; however, the mechanism of the legal protection of personal data was actually launched in 1996 after the entry into force of the Law on Legal Protection of Personal Data, which safeguards the inviolability of an individual's private life in the course of processing personal data.

Until 2010, the legislation did not provide for any entity shaping the personal data protection policy; however, these functions were practically being implemented by the State Data Protection Inspectorate (SDPI). Since 2011, the state policy in the field of data protection has been shaped, organised, coordinated and monitored by the Ministry of Justice. The SDPI has become the institution which takes part in, implements and supervises the personal data protection policy and which is subordinate to the Minister of Justice.

With the rapid advances in information and communication technologies, institutions that shape and implement personal data protection policy have been facing the problem of how to provide favourable conditions for their development and create a secure legal environment that protects an individual's right to privacy.

Over the past few years, a number of legal, management, supervision, information, and methodological issues related to the protection of personal data have piled up in Lithuania, which have not been fully resolved. Therefore, the National Audit Office conducted an audit to assess the efficiency of the protection and supervision of automatically processed personal data and to check whether:

- the regulation of personal data protection conforms to the data processing practices;
- personal data is properly processed at public sector bodies;
- the SDPI performs sufficient supervision of the processing of personal data.

The audit was conducted at the SDPI, data and information was collected at the Ministry of Justice, Ministry of Transport and Communications, Ministry of Health, Ministry of the Interior, Information Society Development Committee under the Ministry of Transport and Communications, and public establishment Central Project Management Agency. The auditors talked to lawyers at the Human Rights Research Institute and law firms SORAINEN and LAWIN, scientists from Mykolas Romeris University, information was also collected at the Office of the Government. The auditors interviewed 108 data controllers / processors and carried out on-the-spot-checks of 20 data controllers / processors as well as analysed the experience and best practices of foreign countries, research data, and information relating to the audited area provided in the mass media

The audit covered the period 2008–2012, which coincided with the economic crisis. Some data from 2013 and earlier periods was also used for analysing trends and changes.

The following public audit conclusions and recommendations were drawn upon the assessment of the audit findings.

CONCLUSIONS

Rapid technological progress determines that more and more personal data is processed by automatic means. The Ministry of Justice and the SDPI should take all measures to properly protect automatically processed personal data; however, the inviolability of an individual's private life and the security level of processed personal data is insufficiently safeguarded due to the following reasons:

1. The legal regulation of personal data protection in Lithuania is in line with the requirements of the European Union, however, it is lagging behind the information and communication technology progress, because the Ministry of Justice and the SDPI are not sufficiently following the internationally accepted principles, methodologies and best practices when formulating the requirements for personal data protection;
2. There is a lack of long-term direction of the personal data protection in the state and clearly formulated personal data protection policy, and the distribution of functions has a number of deficiencies:
   2.1. when shaping the policy for the protection of personal data, the Ministry of Justice has no clear vision for the development of person data protection at the national level and has been focusing on the legislation, rather than the establishment of the priorities in this area and a long-term direction for the protection of personal data;
   2.2. the Ministry of Justice, which also shapes the policy for the protection of personal data and the implementation of the registers managed thereby, as the manager of the main registers in the country, faces a conflict of interest concerning the processing of personal data.
3. The organisation and control of personal data processing in the public sector is not sufficient, because 84 per cent of the inspected institutions do not comply with the legal protection requirements for personal data and only 47 per cent have been properly implementing the data subject's right to privacy. As the data controller, the SDPI has not been complying with all legislative requirements either.
4. The functions implemented by the SDPI lack quality and efficiency, because:
   4.1. in its planning documents, the SDPI has been choosing measures for planning its routine activities, setting targets, assessment criteria and performance indicators for the coming periods the attainment of which depends on the level of activity of data controllers / processors or data subjects;
   4.2. when organising the supervision of data controllers, the SDPI has not been using any risk assessment and management system, preventive inspections and prior checks are usually conducted by way of correspondence, the Inspectorate does not always apply control measures to prevent breaches of data security;
   4.3. the SDPI does not automatically receive data on the automated processing and protection of personal data in the public sector, because this data is collected, for different purposes and by different means, by various institutions which have not aligned their monitoring processes and devices with each other;
   4.4. the methodological guidelines prepared have become obsolete and do not encompass all the problem areas relating to the application of new technologies, the quality of the consulting of data controllers is insufficient, and the information published on the website has been reviewed at irregular intervals;
   4.5. the requirements for the security of personal data in the public sector and general requirements for the security of data (electronic information) have not been aligned and their implementing measures overlap;
   4.6. the electronic services developed by the SDPI until 2013 were unattractive and little used. In 2013 the Inspectorate improved its electronic services and the State Register of Personal Data Controllers; however, not all the improvements have been functioning without obstacles. There is a lack of procedures that would facilitate the provision of electronic services, and the survey instruments that would allow to assess the quality of the electronic services provided by the SDPI have been unreliable;

4.7. the number of publications about personal data protection prepared by the Inspectorate has been going down every year, not all prepared material is updated and made publicly available to the public, so there is untapped potential of new media which could help disseminate information about the protection of personal data or the activities of the institution.

RECOMMENDATIONS

To the Ministry of Justice:

1. In order to properly plan the issues of the legal protection of personal data and to ensure the protection of personal data, the Ministry should:

   1.1. lay down the main directions and targets for developing the legal protection of personal data;

   1.2. clearly separate in its structure the function of shaping the personal data protection policy and the function of implementing the policy of the registers subordinate to the Ministry;

   1.3. improve the monitoring related to the protection of personal data by public bodies in order to easily manage all the necessary information in this field.

To the State Data Protection Inspectorate:

2. In order to improve the quality and efficiency of the regulation of personal data protection, the Inspectorate should reduce the administrative burden on data controllers / processors and organise the supervision of this field more effectively:

   2.1. align the security requirements and procedures for processing personal data in the public sector and general data (information) security requirements and procedures with the Ministry of the Interior;

   2.2. plan the targets and performance indicators for future periods taking into account the guidelines for streamlining the functions of supervisory authorities approved by the Government: rely on more detailed results of surveys of data controllers / processors or their proposals, provide for assessment criteria that would allow measuring changes, etc.;

   2.3. improve the system of the performance, monitoring and risk analysis of the SDPI taking into account all the guidelines for the supervision of economic entities recommended to all supervisory authorities;

   2.4. lay down control measures to ensure the uniform quality of consulting, enhance the reliability of preventive controls, prior checks, and the information provided by the State Register of Personal Data Controllers, and help prevent breaches of data security;

   2.5. prepare methodological materials and recommendations related to the new technologies used in the processing of personal data and more checklists, and to determine an annual procedure for the inspection and revision of the legislation, guidance documents, recommendations, and information published on its website.

3. In order to improve the quality of electronic services and their availability to users, the Inspectorate should:

   3.1. approve a plan and procedures for remedying deficiencies identified in the State Register of Personal Data Controllers and in electronic services, and carry out improvements to facilitate the ordering of services, increase the speed and quality of

the services, reduce the likelihood of errors, and ensure the collection of only accurate and truthful data;

3.2. regularly (at least once a year) assess the use of electronic services and consult with service users on future services of the Register.

4. In order to increase the number of data controllers / processors and data subjects who know well about the protection of personal data, the Inspectorate should develop a three-year plan for preventive action, providing for measures to inform data controllers / processors and data subjects on relevant personal data protection issues, and lay down an annual procedure for the review and updating of the measures envisaged in the plan.