# Effectiveness of internal controls in the protection of personal data in national databases

*Can one be sure that his personal data kept in national registers is protected from abuse?*

**Report of the National Audit Office to the Riigikogu, Tallinn, 25 November 2008**

## Summary of findings

The NAO analysed seven national databases in order to find out how the legitimate use of personal data is ensured. In accordance with the Personal Data Protection Act (hereinafter "PDPA"), the agencies who run databases must ensure that personal data is protected from abuse. The information system of the database must function appropriately, incl. be reliable and safe. Log files must be retained of all instances of viewing, amending, deleting, transmitting of data, etc. These files must allow ex-post determination of who did what, why, when and using which data. In its audit the NAO focused on the functioning of internal controls which must ensure the accuracy and preservation of data and avoid information leaks.

Estonia has been deemed to have a successful e-government where a number of innovative e-services have been introduced. Extensive databases and modern information processing equipment facilitates the work of officials and allows them to provide faster and more convenient services to citizens which usually are also cheaper for them. From time to time, the public has been informed about illegal viewing of data in national databases, and other similar incidents of lesser gravity. Fortunately, these have not created an overall disbelief in e-government and e-services. However, in the worst case, the leakage of personal data may lead to offences against the person, theft of identity or the appreciation of loans and insurances, etc. The first major collapse of national information systems or leakage of sensitive data might suddenly undermine the public's trust, and this in turn could mean setbacks in the development of e-government which some other countries have already experienced.

National registers contain data on all Estonian residents. National as well as private sector databases contain much more personal data than people would expect. In a modern democratic society, one of the fundamental rights of an individual is the right to privacy, and most people would not want information collected on them to be available to others without a good reason. Therefore, it is essential that the agencies who run databases and the data processors employ measures to avoid the access of unauthorised persons to the personal data in the databases, prevent unjustified queries and identify the offender in the case of malicious dissemination of data.

With its audit, the NAO is looking to reinforce the public's confidence that the protection of personal data is not a recent issue but has always been an important matter. The NAO also wishes to support the agencies who run databases in implementing the necessary developments and reorganisation. The third objective of the audit is to draw attention to the fact that, in an e-government, the establishment of good information systems is not enough – the data processors must set up procedures which help to ensure and enable to verify the legitimacy of using personal data.

To safeguard the information entered in the databases, all parties - both data collectors and users as well as the individuals themselves - must be aware of the risks of misusing personal data and the measures for protecting such data. A person has the right to verify the information collected on him and to know who is using his data and for what purpose. If convenient measures are made available to the individual to this end, the individual himself becomes a part of the set of measures implemented for the protection of his data.

The examined internal controls for databases were found to have material deficiencies. Thus, the NAO lacks assurance that personal data in national databases are sufficiently protected from misuse. To improve the situation, the need for effective protection of data entered into databases should be recognised more clearly, the institutions' procedures related to using the databases should be reviewed in the light of the protection of personal data, and regular monitoring of data use should be introduced. Until the above changes are implemented, there cannot be assurance that personal data are protected from unauthorised use or misuse.

**The weakest link of internal controls is the monitoring of data users: log files on the processing of personal data are kept and analysed irregularly, which gives insufficient assurance that the illegal viewing, amending, transmission, etc of data is prevented.** The

agencies who run databases have focused on database security, but in several cases the procedures relating to the protection of personal data have been overlooked. Few agencies have implemented systematic monitoring of the justification of processing personal data in their databases and identified violations. Since most agencies have not implemented checks, the actual extent of illegal processing of personal data is not known. Some of the examined information systems do not allow receiving sufficiently detailed information on the processing of personal data in the database, and the means for monitoring whether such data are used lawfully are insufficient. Other information systems have data which allow monitoring, but this monitoring is not regular – it only takes place following a complaint concerning a suspected violation. Good examples are the procedures of the Ministry of the Interior and the Tax and Customs Board where the random checks of using personal data have become a routine for the Population Register and the Register of Taxable Persons.

In several cases, the chief processor of database has entered into agreements of use with external recipients of data, thereby delegating to them the obligation to ensure the secure and purposeful use of personal data. However, not all of them have shown interest in whether external recipients of data meet these obligations. Unfortunately, it is common that agencies using another one's database do not monitor whether their officials cross-use the databases purposefully.

**The examined databases are lagging behind as regards the introduction of systems securing the information system of the state.** By 1 July 2008, all databases had to conform to a three-level standard security system for information systems to ensure the accessibility of data and protection from unauthorised disclosure and alteration, but in most cases the established schedule was for several reasons not followed. Furthermore, the information systems' data exchange layer (X-Road) has been introduced only partially and the registration of databases in the management system of the national information systems is incomplete. The delayed full-scale introduction of securing systems impedes secure data exchange and the verification of the justification of queries effected through X-Road.

**There is no assurance that effective measures have been employed to protect delicate personal data.** According to the EU Data Protection Directive, the Member States must prohibit the processing of delicate personal data, unless there is a good reason and the security of processing is ensured. Naturally, any risks related to technology and human intervention must be managed when processing such data. Thus, before the processing of delicate personal data begins, a sufficiently secure IT environment must be set up, and all parties handling the data must be informed of their liability. According to the PDPA, the processing of delicate personal data must be registered with the Data Protection Inspectorate or a specific person responsible must be designated to assess compliance with the security requirements for processing delicate personal data in his agency and ensure conformity with the law. The audit showed that access to databases containing delicate data has been provided, but a large number of users, incl. municipalities and educational establishments, have not registered themselves as processors of delicate personal data. Plus, in providing access the chief processors of databases have often ignored whether the external recipients of data have registered the processing of delicate personal data or designated the person responsible for the protection of personal data. Most of the audited municipalities lacked data security documentation and the procedures for using the databases were governed only by the contracts made with the processors of databases. Thus, there is no assurance that effective measures have been employed to protect delicate personal data.

**Individuals are able to find out which data the government has collected on them, but there are no convenient measures to check how the data is used.** A person may submit a request to find out who has viewed his personal data and when and why, but in practice this is rarely done and therefore the public authorities have not focused enough on the creation of IT means to facilitate responding to such requests, let alone solutions where an individual could see already in the state portal whether and how his data have been used. A positive initiative is a solution created by the Citizenship and Migration Board which allows the individuals to see in the state portal who has viewed the data collected on them and when, although this solution does not reflect all the queries at the moment.

**Replies from audited entities:**

**The Estonian Motor Vehicle Registration Centre** agrees to the recommendations given in the draft and adds that the deficiencies mentioned in the audit report will be eliminated once the new information system to be introduced in the first half of 2009 is implemented.

**The Ministry of Economic Affairs and Communications** considers the recommendations concerning the National Traffic Register to be justified and assures that the deficiencies will be eliminated in 2009.

**The Minister of Education and Research** agrees to the audit recommendations and promises to take these into account in the future. At the same time, he informs that some of the deficiencies listed in the draft which were pointed out already in summer 2008 by the Data Protection Inspectorate have been eliminated by the time the audit was completed. The Minister disagrees with the need to sign with

educational establishments and rural municipalities and cities contracts for using the Estonian Education Information System (EHIS).

**The Defence Resources Agency** agrees to the recommendations made. Several recommendations have already been implemented by the time of completing the audit and others have been taken into account in the activities envisaged for 2009 for developing the National Register of Estonian Citizens Liable to Serve in Defence Forces. The Minister of Defence finds that compliance with audit recommendations in 2009 will be highly likely.

**The Tax and Customs Board** agrees to most of the recommendations and describes its positions in detail.

**The Citizenship and Migration Board** agrees to the audit recommendations in general, but points out that the immediate implementation of several recommendations made by the auditors is impeded by the envisaged merger of the Board with the Police Board and the Border Guard Administration in 2010 and the consolidation of ICT of the Ministry of the Interior in the Ministry's IT and Development Centre. Plus, the amount of funds available for next year has dropped and the development work necessary for implementing the audit recommendations is not among the priority tasks of the Board. The Board is of a dissenting opinion as regards the role of the chief processor of a database as comes to registering the processing of delicate personal data with the Data Protection Inspectorate. The Board finds that all contractual external data processors are not required to register the processing of delicate personal data - the respective obligations is put on the chief processor.

**The Minister of Regional Affairs** agrees to the auditors' opinions and informs that several audit recommendations have been already implemented in part. The project for supplementing the Population Register is under way and, in 2009, new and improved monitoring applications will be available; plus, individuals will have access to an e-service which provides information about the queries made on their data to the Population Register.

**The Social Insurance Board** agrees to the audit recommendations in general, but points out that the implementation of several recommendations has been obstructed by the vague division of functions between the Board and the Ministry of Social Affairs. The Board is of a dissenting opinion as regards the mirroring database of the Pension Insurance Register which is accessible to rural municipality and city governments. The Board believes that this is not a separate database and that the access rights of local government bodies do not need to be specified by the chief processor of the register.

**The Minister of Social Affairs** informs that workshops are being held between the Ministry of Social Affairs and the Social Insurance Board to agree on the division of functions related to the National Pension Insurance Register.

**The Data Protection Inspectorate** informs that it will analyse in depth the audit recommendations to develop additional guidelines and where necessary include these in the work plan for 2009.

**The audited municipalities** agree to the auditors' opinions in general and promise to take the recommendations into account. Most of the local government bodies undertake to supplement the current internal rules of procedure with provisions on password management and monitoring arrangements.

Before the completion of the audit, the municipalities of Anija and Kanepi have appointed the person responsible for the protection of personal data, others have initiated procedures for appointing the person responsible or registering the processing of delicate personal data at the Data Protection Inspectorate.

For verifying the justification of queries related to personal data, most audited municipalities have introduced or are in the process of introducing the application form for queries. The municipalities of Torma and Antsla find that for the subsequent monitoring of using the registers there could be a uniform registration system, or a place for entering the reason for the query in the information system of the national register itself.

Ülle Madise
Director of Audit
Audit Department II