Translation from Lithuanian

MINISTER OF THE INTERIOR OF THE REPUBLIC OF LITHUANIA
O R D E R

ON THE APPROVAL OF DATA SAFETY REGULATIONS OF THE DEPARTMENTAL REGISTER OF SUSPECTED, ACCUSED AND CONVICTED PERSONS

23 December 2005, No. 1V-429
Vilnius

In accordance with paragraph 3 of Article 20 of the Republic of Lithuania Law on State Registers (Official Gazette *Valstybės žinios*, 1996, No. 86-2043; 2004, No. 124-4488),

I hereby a p p r o v e the Data Safety Regulations of the Departmental Register of Suspected, Accused and Convicted Persons (enclosed).

MINISTER OF THE INTERIOR GINTARAS FURMANAVIČIUS

_____

APPROVED
Minister of the Interior of the
Republic of Lithuania
Order No. 1V-429
of 23 December 2005

DATA SAFETY REGULATIONS OF THE DEPARTMENTAL REGISTER OF SUSPECTED, ACCUSED AND CONVICTED PERSONS

I. GENERAL PROVISIONS

1. The purpose of the Data Safety Regulations of the Departmental Register of Suspected, Accused and Convicted Persons (hereinafter – the Safety Regulations) shall be to enable safe automated processing of the data contained in the Departmental Register of Suspected, Accused and Convicted Persons (hereinafter – the Register).

2. The Safety Regulations shall regulate automated data processing in the Register and shall be mandatory to all civil servants and employees working under employment contracts in the register management institution (hereinafter – users of the Register).

3. The Safety Regulations together with the regulations of safe data handling, the contingency management plan, the risk report, detailed guidelines and procedure descriptions define the safety policy of the Register (hereinafter – the safety policy).

II. DESCRIPTION OF THE REGISTER

4. Description of the Register:

4.1. Purpose of the Register is to register the objects of the Register, gather, compile, process, systemise, store, use and provide Register data and documents to pre-trial investigation institutions, courts, other public authorities and institutions, natural and legal persons, and perform other actions of processing Register data;

4.2. Objects of the Register are suspected, accused and convicted persons:

4.2.1. Natural and legal persons summoned a notice on suspicions (instituted criminal proceedings);

4.2.2. Natural persons accused in private accusation proceedings (accused in criminal proceedings instituted only as a result of the victim's complaint);

4.2.3. Natural and legal persons to be prosecuted upon the decision of the court or whose sentences are to be varied or annulled;

4.2.4. Natural persons with ongoing enforcement of judgments of conviction and rulings in criminal proceedings;

4.3. Register data shall not be subject to public disclosure.

5. The Register consists of legal, organisational and technological measures designated to gather, compile, process, systemise, store, provide data and carry out other actions of processing the register. All data processed in the Register shall be classified by data groups.

6. The Register processes the following data groups specified in the Regulations of the Register:

6.1. General data of Register objects;

6.2. Data on pre-trial investigation (instituted criminal proceedings) and private accusation proceedings (accused in criminal proceedings instituted only as a result of the victim's complaint);

6.3. Data on imposed remand measures;

6.4. Data on decisions passed after hearing criminal cases and on amending decisions;

6.5. Data on the enforcement of sentences imposed upon natural persons.

7. Safe processing of register data is regulated by:

7.1. Republic of Lithuania Law on the Legal Protection of Personal Data (Official Gazette *Valstybės žinios*, 1996, No. 63-1479; 2003, No. 15-597);

7.2. Republic of Lithuania Law on State Registers (Official Gazette *Valstybės žinios*, 1996, No. 86-2043; 2004, No. 124-4488);

7.3. General data safety requirements, approved by Resolution No. 952 of the Government of the Republic of Lithuania on 4 September 1997 (Official Gazette *Valstybės žinios*, 1997, No. 86-2075; 2003, No. 2-45);

7.4. Regulations of the Departmental Register of Suspected, Accused and Convicted Persons, approved by Order No. 1V-291 of the Minister of the Interior of the Republic of Lithuania on 13 September 2005 (Official Gazette *Valstybės žinios*, 2005, No. 112-4114);

7.5. Lithuanian Standard LST ISO/IEC 17799:2005, Lithuanian and international standards of group "Information Technologies. Safety Equipment", regulating safe data processing;

7.6. Other legal acts regulating the legitimacy of data processing, activities of the register management institution and the management of data safety.

III. ORGANISING OF DATA SAFETY AND CONTINGENCY MANAGEMENT

8. The Register management institution shall be responsible for the legitimacy of processing of Register data and data safety.

9. IT and Communications Department under the Ministry of the Interior of the Republic of Lithuania shall be a representative for data safety of the Register (hereinafter – Safety Representative) to be in charge of implementing and controlling the data safety policy of the Register.

10. The Safety Representative shall appoint an administrator of the Register who shall report for the performance of the assigned functions directly to the Safety Representative.

11. Register users shall have adequate qualification (professional development courses of IT users, initial training on data handling, ECDL user certificate, etc.) and experience of work with applications. Register users shall have knowledge of the documents regulating data processing and data use.

12. The administrator shall have knowledge of the key principles of safety policy, work with computer networks, ensure their safety, have experience in the administration and maintenance of operating systems (*Windows*, *Unix, Oracle*).

13. Register users, upon noticing any infringements of the safety policy, elements of criminal offences, inoperative or improperly operating protective measures of data safety shall immediately make a notice to the administrator that shall inform the Safety Representative thereabout and in case there is no administrator, a notice shall be made to the Safety Representative.

14. The actions of Register users in contingency situations shall be regulated by the contingency management plan to be submitted for approval of the Minister of the Interior by the Safety Representative. The primary provisions of the plan: protection of life and health of users, recovery of the Register activities, training of Register users.

IV. RISK ASESSMENT AND DETAILED WORK PROCEDURES

15. Major risk mitigation measures shall be set forth in the risk report, which shall be approved by the Minister of the Interior and drawn up by the Safety Representative after taking into consideration any identified risk factors, i.e. subjective unintentional (data processing errors and mistakes, data deletion, mistaken provision of data, physical failures of IT software errors, etc.), subjective deliberate (unauthorised use of the Register to obtain data, data replacement or destruction, theft of IT, etc.) and force majeure (events laid down in paragraph 3 of the Regulation on release from liability in case of *force majeure*, approved by Resolution No. 840 of the Government of the Republic of Lithuania on 15 July 1996 (Official Gazette *Valstybės žinios*, 1996, No. 68-1652)).

16. Specific register data processing and safety procedures shall be specified in detailed data handling regulations to be submitted for approval of the Minister of the Interior by the Safety Representative.

V. LIABILITY OF REGISTER USERS

17. Register users shall take care of the safety of the Register and the data processed therein.

18. Register data may be processed only by the Register users who have familiarised themselves with the Safety Regulations and other legal acts regulating the safety policy and have agreed in writing to abide by the requirements of these legal acts.

19. Register users shall be briefed about the Safety Regulations and other legal acts regulating the safety policy as well as about their liability for failure to follow such requirements against signature by the Safety Representative. Register users shall also be informed in writing about amendments to the Safety Regulations or revocation, amendments or enacting of other legal acts regulating the safety policy.

20. Register users shall be offered regular training on data safety, reminded about the topics of safety in different forms (e.g. reminders by e-mail, specific seminars, guides to newly recruited employees, etc.).

21. Register users who violate the requirements of the Safety Regulations and other legal acts regulating the safety policy shall be liable under the procedure prescribed by laws.

VI. PROCEDURE FOR UPDATING THE SAFETY REGULATONS

22. In order to ensure the safety of the Register and the data processed therein, the Safety Representative shall provide recommendations to the Minister of the Interior on amendments to the Safety Regulations or on the adoption, amendment or revocation of other legal acts regulating the safety policy.

23. The Safety Regulations and other legal acts regulating the safety policy shall be revised in substance by carrying out an audit referred to in paragraph 24 hereof at least once a year or more often, if necessary.

VII. FINAL PROVISIONS

24. In order to ensure the control over implementation of the provisions contained in the Safety Regulations and other legal acts regulating the safety policy, the Safety Representative shall arrange an annual audit:

24.1. To assess the compliance of the Safety Regulations and other legal acts regulating the safety policy to the actual safety;

24.2. To take inventory of the technical equipment and software of the Register;

24.3. To inspect not less than 10 per cent of the workstations of the Register users and the applications and their configuration installed in all service computers;

24.4. To audit the compliance of the rights granted to the Register users and the functions they perform and extend or limit their functions accordingly;

24.5. To assess the readiness to recover the Register activities in case of emergencies.

25. The audit shall be followed by the plan of elimination of identified shortcomings; the plan shall be approved, persons in charge shall be appointed and implementation time-limits shall be set by the Minister of the Interior.

_____