/Translation from Lithuanian/

ORDER
OF THE MINISTER OF THE INTERIOR OF THE REPUBLIC OF LITHUANIA

REGARDING THE DEPARTMENTAL REGISTER OF WANTED PERSONS, UNIDENTIFIED BODIES AND UNKNOWN HELPLESS PERSONS

20 June 2006 No. 1V-232
Vilnius

Following Article 6(5) and Article 20(3) of the Law of the Republic of Lithuania on State Registers (*Official Gazette*, 1996, No. 86-2043; 2004, No. 124-4488):

1. I hereby establish the Departmental Register of Wanted Persons, Unidentified Bodies and Unknown Helpless Persons based on the Wanted Persons central database managed in accordance with the Instructions for Search of Persons approved by Order No. 4RN of the Minister of the Interior of the Republic of Lithuania of 16 July 2003 and with the Instructions for Personal Identification of Unidentified Bodies, Unknown Patients or Unknown Children approved by Order No. 714/153/562 of the Minister of the Interior of the Republic of Lithuania, the Prosecutor General of the Republic of Lithuania and the Minister of Health of the Republic of Lithuania of 29 December 1999 (*Official Gazette*, 2000, No. 2-53).

2. I hereby approve the hereto attached:

2.1. Regulations of the Departmental Register of Wanted Persons, Unidentified Bodies and Unknown Helpless Persons;

2.2. Regulations of Data Security of the Departmental Register of Wanted Persons, Unidentified Bodies and Unknown Helpless Persons.

3. I hereby set the date of commencement of functioning of the Departmental Register of Wanted Persons, Unidentified Bodies and Unknown Helpless Persons – 1 January 2007.

4. I hereby assign the Information and Communications Department under the Ministry of the Interior of the Republic of Lithuania in due course before the commencement of functioning of the Departmental Register of Wanted Persons, Unidentified Bodies and Unknown Helpless Persons:

4.1. to draft and submit to the Minister of the Interior draft detailed instructions of working with the data of the Departmental Register of Wanted Persons, Unidentified Bodies and Unknown Helpless Persons, draft procedure description and draft rules for secure data handling;

4.2. to organise the development of programme measures required for handling data of the Departmental Register of Wanted Persons, Unidentified Bodies and Unknown Helpless Persons.

MINISTER OF THE INTERIOR AD INTERIM GINTARAS FURMANAVIČIUS

APPROVED
by Order No. 1V-232 of the Minister of the Interior
of the Republic of Lithuania of 20 June 2006

REGULATIONS OF THE DEPARTMENTAL REGISTER OF WANTED PERSONS, UNIDENTIFIED BODIES AND UNKNOWN HELPLESS PERSONS

I. GENERAL PROVISIONS

1. The Regulations of the Departmental Register of Wanted Persons, Unidentified Bodies and Unknown Helpless Persons (hereinafter referred to as the Regulations) shall regulate the purpose of the Departmental Register of Wanted Persons, Unidentified Bodies and Unknown Helpless Persons (hereinafter referred to as the Register) – a part of the information system of the Ministry of the Interior), the Register objects, institutions managing the Register, rights and duties thereof, management, reorganisation and liquidation of the Register.

2. The purpose of the Register shall be to register objects of the Register, to collect, accumulate, process, systemise, store and provide the Register data and to perform other actions of handling the Register data.

3. Objects of the Register:

3.1. wanted persons;

3.2. unidentified bodies found;

3.3. unknown helpless persons found being identified.

4. The purpose of handling personal data of the Register shall be organisation and performance of search of persons and identification of unidentified bodies and unknown helpless persons.

5. The Register data shall be accumulated in the single database of the Register.

6. Data to the Register shall be submitted by pre-trial investigation authorities and other public institutions and authorities referred to in paragraph 21 hereof.

7. The Register shall be managed following:

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

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

7.3. the Law of the Republic of Lithuania on Police Activities (*Official Gazette*, 2000, No. 90-2777);

7.4. the Regulations and other legal acts regulating the management of the Register.

8. For the purpose hereof the following concepts shall be used:

Wanted person shall mean a hiding or wanted natural person whose location is unknown and with regard to whom the interior statutory authorities perform search actions in the territory of the Republic of Lithuania on legally stipulated grounds and in accordance with the legally set procedure.

Unidentified body shall mean a human body or skeleton found in the Republic of Lithuania or a patient dying in a health care institution whose identity is not established on the grounds of objective data.

Unknown helpless person shall mean a patient or child found in the Republic of Lithuania who because of their health condition or age are helpless and cannot provide any data about themselves and whose identity is not established on the grounds of objective data

II. AUTHORITIES MANAGING THE REGISTER

9. The Managing Authority managing the Register shall be the Ministry of the Interior of the Republic of Lithuania (hereinafter referred to as the Ministry of the Interior).

10. Authorities managing the Register:

10.1. the Information and Communications Department under the Ministry of the Interior of the Republic of Lithuania (hereinafter referred to as the Information and Communications Department);

10.2. territorial and specialised police departments (hereinafter referred to as police departments);

10.3. the State Border Guard Service under the Ministry of the Interior of the Republic of Lithuania (hereinafter referred to as the State Border Guard Service).

11. The Managing Authority managing the Register shall:

11.1. methodologically manage the Register, coordinate and control the work of authorities managing the Register;

11.2. approve legal acts related to the Register management and security of the Register data and enforce observance thereof;

11.3. organise procurement, installation and modernisation of hardware and software to manage the Register;

11.4. execute agreements on provision of data to the Register;

11.5. organise and coordinate professional development of civil servants and employees employed under employment contracts handling the Register data (hereinafter referred to as persons handling the Register data) of authorities managing the Register;

11.6. consider proposals of authorities managing the Register regarding improvements of the Register functioning and summarise them;

11.7. ensure that the Register would be managed in accordance with the Law of the Republic of Lithuania on State Registers, the Regulations and other legal acts;

11.8. provide information about the activity of the Register to stakeholders;

11.9. perform other functions stipulated and assigned thereto in the Regulations and other legal acts.

12. The Managing Authority managing the Register shall be the manager of personal data of the Register.

13. The Information and Communications Department shall:

13.1. organise and coordinate or perform the works to support and update hardware and software of the Register;

13.2. ensure security of the Register data;

13.3. within its competence support data transmission networks of the Register;

13.4. organise the interaction of the Register with other registers and information systems;

13.5. enter data received in the case referred to in paragraph 22 of the Regulations into the Register database;

13.6. prepare statistical data about wanted persons, unidentified bodies and unknown helpless persons and submit it to the Police Department under the Ministry of the Interior of the Republic of Lithuania;

13.7. provide the Register data in accordance with the procedure laid down in the Regulations, agreements and other legal acts;

13.8. check distinctive marks of unidentified bodies and unknown helpless persons against distinctive marks of wanted persons;

13.9. perform other functions stipulated in the Regulations and other legal acts.

14. Police departments shall register the Register objects in accordance with the procedure laid down in the Instructions for Search of Persons approved by Order No. 4RN of the Minister of the Interior of the Republic of Lithuania of 16 July 2003, the Instructions for Personal Identification of Unidentified Bodies, Unknown Patients or Unknown Children approved by Order No. 714/153/562 of the Minister of the Interior of the Republic of Lithuania, the Prosecutor General of the Republic of Lithuania and the Minister of Health of the Republic of Lithuania of 29 December 1999 (*Official Gazette*, 2000, No. 2-53) and the Regulations.

15. The State Border Guard Service shall register objects of the Register in accordance with the procedure laid down in the Instructions for Search of Persons and the Regulations.

16. Authorities managing the Register shall ensure proper functioning of the Register and security of data and documents.

17. Authorities managing the Register must ensure that:

17.1. the Register would function without interruption;

17.2. the Register data would match the data specified in documents submitted to the authority managing the Register;

17.3. the Register data received from related registers would be continuously updated;

17.4. incorrect, inaccurate and incomprehensive data of the Register or changes to the Register data would be immediately corrected, updated or supplemented;

17.5. recipients of the Register data to whom incorrect, inaccurate and incomprehensive data of the Register is transmitted would be informed about any imprecision corrected;

17.6. the Register would be managed in accordance with the Regulations and other legal acts.

18. Authorities managing the Register shall be entitled:

18.1. to demand from providers of the Register data that the register data, changes thereto and documents would be properly drafted, submitted in time and match the data in related registers;

18.2. to set a period of time for the provider of the Register data to remove any faults where the authority managing the Register establishes that data or documents submitted to the Register are inaccurate or do not meet the requirements laid down in legal acts;

18.3. to set principle and procedure of organising the work of the Register;

18.4. to perform other actions stipulated in the Regulations.

19. Authorities managing the Register shall be managers of personal data of the Register.

III. REGISTER DATA

20. Register data:

20.1. programmed identification code of the wanted person, unidentified body or unknown helpless person;

20.2. personal data of the wanted person:

20.2.1. category of the wanted person: the person wanted is a suspect, an accused, wanted, a debtor or a defendant;

20.2.2. photograph;

20.2.3. personal code;

20.2.4. name;

20.2.5. surname;

20.2.6. date of birth;

20.2.7. sex;

20.2.8. number and date of issue and validity of the personal identification document;

20.2.9. measure of restraint (type, date of imposition);

20.2.10. declared place of residence or the last known place of residence;

20.3. data of the search case, pre-trial investigation or criminal case (if initiated), personal identification case:

20.3.1. category code of the wanted person in accordance with the Instructions for Search of Persons;

20.3.2. the public institution or authority performing search or personal identification actions (name, code) in accordance with Annex 6 of the Instructions for Centralised Accounting of Criminal Acts, Persons Having Committed Them and Victims Thereof approved by Order No. 1V-160 of the Minister of the Interior of the Republic of Lithuania of 8 May 2003 (*Official Gazette*, 2003, No. 50-2230);

20.3.3. number of the search case, date of initiating the search case;

20.3.4. number of the criminal case, date of starting the pre-trial investigation, number of the article of the Criminal Code of the Republic of Lithuania (*Official Gazette*, 2000, No. 89-2741) providing for a criminal offence whereof the wanted person is suspected, accused or sentenced;

20.3.5. number of the personal identification case, date of initiating the personal identification case;

20.4. identification data of the wanted person, unidentified body or unknown helpless person:

20.4.1. category of the person: the person wanted is a suspect, an accused, a culprit, wanted, a debtor, a defendant, an unknown helpless person or an unidentified body;

20.4.2. appearance is European, Asian, Roma, Caucasian, etc.;

20.4.3. reference of the fingerprint card in the Automated Fingerprint Identification Register of the Lithuanian Police;

20.4.4. age judging by the appearance;

20.4.5. date of disappearance and finding;

20.4.6. place of disappearance and finding;

20.4.7. circumstances of disappearance;

20.4.8. anticipated location of the wanted person;

20.4.9. time of death (how may hours, days, weeks, months, years ago);

20.4.10. cause of death;

20.4.11. condition of the body;

20.4.12. date of the body autopsy/date of medical examination of the unknown helpless person;

20.4.13. time and place of burial, number of the grave;

20.4.14. height, length of the body;

20.4.15. head size, head circumference;

20.4.16. foot size;

20.4.17. distinctive body marks;

20.4.18. DNA analyte (genotype) reference in the DNA Register of the Lithuanian Police;

20.4.19. teeth condition scheme;

20.4.20. external features;

20.5. other data:

20.5.1. date of receipt of a statement or notice about a wanted person at a police department;

20.5.2. date of announcing the search;

20.5.3. legal grounds and date of terminating the search;

20.5.4. legal grounds and date of terminating the personal identification case;

20.5.5. date of entering data into the Register database;

20.5.6. name, surname and position of the person managing the search case or the personal identification case;

20.5.7. name/name and surname of the search initiator.

IV. REGISTRATION OF THE REGISTER OBJECTS

21. The Register data shall be provided by:

21.1. the Military Police of the Lithuanian Army;

21.2. the Special Investigation Service of the Republic of Lithuania;

21.3. the Criminal Service of the Customs;

21.4. the National Security Department of the Republic of Lithuania as a pre-trial investigation authority;

21.5. the Prosecutor General’s Office and territorial prosecutors’ offices;

21.6. courts;

21.7. healthcare institutions;

21.8. the Financial Crime Investigation Service under the Ministry of the Interior of the Republic of Lithuania (hereinafter referred to as the Financial Crime Investigation Service);

21.9. the Fire and Rescue Department under the Ministry of the Interior of the Republic of Lithuania (hereinafter referred to as the Fire and Rescue Department).

22. The public institutions and authorities listed in paragraphs 21.1-21.4 hereof shall immediately after announcing the search for a person provide a written notice stating the data specified in paragraphs 20.2-20.4 (except for paragraphs 20.4.3 and 20.4.18), 20.5.2 and 20.5.7 hereof, and after terminating the search for the person – a written notice stating the data specified in paragraphs 20.2.1, 20.2.3-20.2.6, 20.3.2, 20.3.3, 20.5.3 and 20.5.7 hereof to the Information and Communications Department, and the latter shall immediately verify the data against data of related registers and enter it into the Register database.

23. The public authorities and institutions listed in paragraphs 21.5, 21.6, 21.8 and 21.9 hereof shall immediately provide a notice with the data listed in paragraphs 20.2, 20.5.2 and 20.5.7 hereof together with the prosecutor’s resolution or a court ruling to announce the search for a person to territorial police departments that shall immediately verify the data against data of related registers and enter it into the Register database.

24. Health care institutions shall provide the identification data document of the form specified in the Instructions for Identification of an Unidentified Body, Unknown Patient or Unknown Child with data of the unidentified body or unknown helpless person listed in paragraphs 20.4.1, 20.4.2, 20.4.4-20.4.6, 20.4.9-20.4.12, 20.4.14-20.4.17, 20.4.19, 20.4.20 and 20.5.7 hereof to territorial police departments on the date of drafting the forensic examination certificate or on the date of finding or admitting the unknown helpless person to the health care institution, and territorial police departments shall immediately verify the data against data of related registers and enter it into the Register database.

25. Providers of the Register data shall be responsible for correctness, accuracy and comprehensiveness of the data submitted to the Register.

26. Police departments shall fill the Register database with the data of a wanted person, unidentified body or unknown helpless person and other data listed in paragraph 20 hereof received from bailiffs and correction inspectorates or otherwise collected when performing direct search functions.

27. The State Border Guard Service shall fill the Register database with the data of a wanted person, data of personal identification and search cases listed in paragraphs 20.2-20.4 and other data specified in paragraphs 20.5.2, 20.5.3, 20.5.5-20.5.7 hereof received when performing direct search functions.

28. Police departments and the State Border Guard Service shall fill the Register database with the data listed in paragraphs 20.2-20.4, 20.5.1-20.5.3 and 20.5.5-20.5.7 immediately:

28.1. following the initiation of the search case;

28.2. having received a notice on a wanted person;

28.3. having announced search where the search case is not initiated;

28.4. having terminated the search for a wanted person.

29. Police departments shall enter the data listed in paragraphs 20.3.2, 20.3.5, 20.4 and 20.5.5-20.5.7 hereof into the Register database no later than within 10 days following the day of finding an unidentified body or an unknown helpless person and data specified in paragraph 20.5.4 hereof – following the date of adopting a resolution to terminate the personal identification case.

30. The Register object shall be deemed registered where the data specified in paragraph 20 hereof is entered into the Register database and the identification code is assigned to the object being registered.

31. Having established that the data submitted by the data provider is inaccurate, within 3 working days following the date of becoming aware of inaccuracy the authority managing the Register shall inform the data provider accordingly in writing and demand to correct the inaccuracy. The provider of the Register data shall be obliged within 5 working days following the receipt of the request to correct inaccuracy to submit specified data of the Register to the authority managing the Register. Only after the data provider specifies the data, the authority managing the Register shall enter it into the Register database.

32. Providers of the Register data having familiarised themselves with the Register data provided thereby and established that incorrect, inaccurate or incomprehensive data is entered into the Register database shall be entitled to demand that the incorrect data would be corrected, the incomprehensive or inaccurate data would be supplemented and the unnecessary or illegitimately collected data of the Register would be deleted. The authority managing the Register shall be obliged within 5 working days following the receipt of the request and documents certifying the facts specified therein to fulfil the request and inform the data provider accordingly.

33. Providers of the Register data shall immediately inform the authority managing the Register of any changes to the data submitted to the Register. Having received a written notice of the provider of the Register data about changes to the data of the Register object, the authority managing the Register shall within 5 working days following the receipt of the request and documents certifying the facts specified therein change the data in the Register database.

34. Having established any lack of correspondence between the data received from a related register and the data submitted by the data provider, the authority managing the Register must immediately in writing inform the provider of the Register data accordingly. The provider of the Register data shall be obliged within 5 working days following the receipt of the notice about inaccuracy of data to submit specified data or explanations of circumstances to the authority managing the Register. Having established inaccuracy of data of a related register or after the data provider specifies this data, the authority managing the Register shall enter it into the Register database.

35. The person whose data is entered into the Register shall be entitled to familiarise themselves with their data handled within the Register subject to presenting their personal identification document. The authority managing the Register shall present them the data within 10 working days following the day of address by the person.

36. Within 5 working days following the receipt of a written request of the person whose data is handled within the Register to correct incorrect, inaccurate and incomprehensive data or to delete illegitimately collected data and documents certifying the facts given therein, the authority managing the Register shall correct the Register data or delete the illegitimately collected data and inform the person having so requested in writing.

37. Having established that incorrect, inaccurate and incomprehensive data has been entered into the Register database through its fault, no later than within 3 working days following the date of becoming aware of such circumstances, the authority managing the Register must correct inaccuracies and free of charge inform all recipients of the Register data in writing that incorrect, incomprehensive and inaccurate data has been provided to them.

38. After termination of a case of search for a person or personal identification case, the Information and Communications Department shall delete the Register objects from the Register at the beginning of each year but no later than by 10 January.

39. The Information and Communications Department shall immediately move the data of objects deleted from the Register database to the archive of the Register database. In the database archive data shall be stored after termination of a search case or personal identification case:

39.1. for 1 year where the search for a wanted person is terminated after the wanted person is found or detained or where their location is identified, after terminating the pre-trial investigation or after the court makes a ruling to terminate the execution of the decision and to terminate the search for such a person or after establishing the fact of death of the wanted person;

39.2. for 15 years where the search for a wanted person is terminated on other grounds not listed in paragraph 39.1 hereof;

39.3. for 5 years where the personal identification case is terminated upon identifying the unidentified body or unknown helpless person;

39.4. for 15 years where the personal identification case is terminated upon failure to identify the unidentified body or unknown helpless person.

40. Following the expiry of the term of storage of the Register data in the Register database archive, the Information and Communications Department shall immediately destroy the Register data.

V. INTERACTION WITH OTHER REGISTERS

41. Data of the following related registers shall additionally be used for describing the Register objects:

41.1. the Register of Residents of the Republic of Lithuania – data specified in paragraphs 20.2.3-20.2.8, 20.2.10 and 39.1 hereof;

41.2. the Departmental Register of Suspected, Accused and Convicted Persons – data specified in paragraph 20.2.9 hereof;

41.3. the Register of Automated Fingerprint Identification of the Lithuanian Police – data specified in paragraph 20.4.3 hereof;

41.4. the DNA Register of the Lithuanian Police – data specified in paragraph 20.4.18 hereof.

42. The Register data shall be classified using codes of pre-trial investigation institutions given in Annex 6 to the Instructions for Centralised Accounting of Criminal Acts, Persons Having Committed Them and Victims Thereof.

43. Data shall be received from related registers automatically.

44. Having established that data received from a related register is inaccurate, the authority managing the Register must immediately in writing transmit incorrect, inaccurate and incomprehensive data and explanations of circumstances to the authority managing the related register.

45. Having received information about inaccuracies established in the data transmitted to a related register and explanations of circumstances from such a register, within 3 working days following the date of receipt of the information the authority managing the Register must check the information provided and where it is confirmed correct the inaccuracy. Where the authority managing the Register must contact the data provider for correcting inaccuracies, this term shall be extended for 5 more working days.

46. Having corrected the inaccurate data of the Register, the authority managing the Register shall immediately in writing inform the authority managing the related register and recipients of the Register data to whom incorrect, inaccurate and incomprehensive data has been transmitted.

VI. PROVISION AND USE OF THE REGISTER DATA

47. The Register data shall be provided to data recipients entitled to receive it in accordance with the procedure laid down in the laws and other legal acts of the Republic of Lithuania:

47.1. when issuing certificates or other documents;

47.2. when issuing extracts from the Register and providing other information that may be provided verbally, in writing, by e-mail or other means of communication;

47.3. automatically;

47.4. by other statutory means.

48. Data shall be provided to data recipients on the grounds of a single application specifying the purpose of data use or on the grounds of data provision agreements (in the event of multiple provision) specifying the Register data provided, the purpose, conditions and procedure of use thereof.

49. The Register data shall be provided free of charge:

49.1. to natural persons – their data handled within the Register once per calendar year;

49.2. to law-enforcement institutions and courts – for performance of their direct functions;

49.3. to units of the administration of the Ministry of the Interior, institutions under the Ministry of the Interior and the State Enterprise Regitra – for performance of their direct functions;

49.4. to the Second Department of Operational Services under the Ministry of National Defence of the Republic of Lithuania – for performance of their direct functions;

49.5. to data providers not listed in paragraphs 49.2 and 49.3 hereof – only data provided thereby and entered into the Register;

49.6. in other cases stipulated in Article 17(4) of the Law of the Republic of Lithuania on State Registers.

50. Other data recipients not listed in paragraph 49 hereof shall be provided the Register data for a fee whose size shall be calculated in accordance with the Description of the Procedure for Establishing the Size of Remuneration for Provision of State Register and Cadastre Data approved by Resolution No. 739 of the Government of the Republic of Lithuania of 30 June 2005 (*Official Gazette*, 2005, No. 82-3024).

51. Having noticed that data transmitted is inaccurate, recipients of the Register data shall immediately inform the authority managing the Register thereof. Within 10 working days following the date of receipt of information about the Register data inaccuracies, the authority managing the Register must check the information provided and where it is confirmed correct inaccuracies and inform the data recipient thereof in writing, and where the information is not confirmed – inform the recipient of the Register data having provided information about the refusal to correct inaccuracies in writing.

VII. TRANSMISSION OF THE REGISTER DATA TO FOREIGN COUNTRIES

52. The Register data shall be provided to legal and natural persons of the European Union Member States in accordance with the same procedure as the one applicable to legal and natural persons of the Republic of Lithuania.

53. The Register data shall be provided to legal and natural persons of third countries in accordance with the laws and other legal acts of the Republic of Lithuania and international treaties.

VIII. PROTECTION OF THE REGISTER DATA

54. Security of the Register data is regulated by the Regulations of Security of the Register Data that together with detailed instructions, procedure descriptions and the Rules for Secure Data Handling shall define the security policy of the Register.

55. All authorities managing the Register shall be responsible for security of the Register data.

56. The Managing Authority managing the Register shall be responsible for:

56.1. preparing the central computer premises with limited access;

56.2. functioning of the system of permits to handle data for persons managing the Register data;

56.3. preparing the storage for backup copies of the operation system, database and database archive.

57. The Information and Communications Department shall register the Register data recipients and persons managing the Register data and grant rights to handle the Register data in accordance with the procedure laid down by the Minister of the Interior of the Republic of Lithuania.

58. Only duly authorised persons managing the Register data shall be entitled to enter the Register data into the Register database or correct it.

59. The software tools of data protection must meet the following requirements:

59.1. every person managing the Register data must be uniquely identified;

59.2. a system of passwords must be implemented;

59.3. all computer operations related to the Register data handling and attempts to perform them shall be registered;

59.4. systemware and applications must ensure the Register data invulnerability.

60. Persons managing the Register data must sign a commitment to keep data a secret for a period of time stipulated in the laws and other legal acts and not to violate the Law of the Republic of Lithuania on Legal Protection of Personal Data. The person shall be liable for illegitimate disclosure, transmission, change or deletion of the Register data according to the procedure established by the laws.

IX. REGISTER FUNDING

61. The Register shall be funded by the state budget of the Republic of Lithuania, the funds received for services provided and financial sources specified in other legal acts.

X. REORGANISATION AND LIQUIDATION OF THE REGISTER

62. The Register shall be reorganised and liquidated in accordance with the procedure laid down in the legal acts.

63. Documents and data of the Register being liquidated shall be transferred to another state or departmental register, deleted or transferred to state archives in accordance with the procedure laid down in the Law of the Republic of Lithuania on Documents and Archives (*Official Gazette*, 1995, No. 107-2389; 2004, No. 57-1982).

COORDINATED
Minister of National Defence of the Republic of Lithuania
Gediminas Kirkilas
30 May 2006

COORDINATED
Minister of Justice of the Republic of Lithuania
Gintautas Bužinskas
29 May 2006

COORDINATED
Minister of Finance ad interim
of the Republic of Lithuania
Zigmantas Balčytis
12 June 2006

COORDINATED
Minister of Health ad interim
of the Republic of Lithuania
Žilvinas Padaiga
2 June 2006

COORDINATED
Director General of the National Security
Department of the Republic of Lithuania
Arvydas Pocius
13 June 2006

COORDINATED
Deputy Director of the National Court
Administration
Romas Laurinavičius
14 June 2006

COORDINATED
Director of the Special Investigation Service of the Republic of Lithuania
Povilas Malakauskas
12 June 2006

COORDINATED
Prosecutor General of the Republic of Lithuania
Algimantas Valantinas
19 June 2006

____

APPROVED
by Order No. 1V-232 of the Minister of
the Interior of the Republic of Lithuania
of 20 June 2006

REGULATIONS OF THE DATA SECURITY OF THE DEPARTMENTAL REGISTER OF WANTED PERSONS, UNIDENTIFIED BODIES AND UNKNOWN HELPLESS PERSONS

I. GENERAL PROVISIONS

1. The purpose of the Regulations of the Data Security of the Departmental Register of Wanted Persons, Unidentified Bodies and Unknown Helpless Persons (hereinafter referred to as the Security Regulations) shall be to create conditions for secure automated handling of the data of the Departmental Register of Wanted Persons, Unidentified Bodies and Unknown Helpless Persons (hereinafter referred to as the Register).

2. The Security Regulations shall regulated automated processing of data in the Register and shall be binding on all civil servants and employees employed under employment contracts in authorities managing the Register (hereinafter referred to as the Register users).

3. The Security Regulations are drafted following the General Data Security Requirements approved by Resolution No. 952 of the Government of the Republic of Lithuania of 4 September 1997 (*Official Gazette*, 1997, No. 83-2075; 2003, No. 2-45), the Typical Data Security Regulations approved by Order No. 1V-272 of the Minister of the Interior of the Republic of Lithuania of 16 July 2003 (*Official Gazette*, 2003, No. 76-3511) and other legal acts regulating legitimacy of data handling, activities of authorities managing the Register and data security management.

II. DESCRIPTION OF THE REGISTER

4. The purpose of the Register shall be to register objects of the Register and handle the Register data.

5. Objects of the Register shall be wanted persons, unidentified bodies and unknown helpless persons found being identified.

6. The Register data shall not be publicly disclosed.

7. The Register shall contain legal, organisational and technical means to collect, accumulate, process, systemise, store and provide data and to perform other actions of handling the Register data. All data handled in the Register shall be classified by data groups.

8. The Register shall handle the following data groups:

8.1. data of the wanted person:

8.2. data of the search file, pre-trial investigation or criminal case (if initiated), personal identification file;

8.3. identification data of the wanted person, unidentified body or unknown helpless person;

8.4. identification code of the Register object;

8.5. other data.

III. ORGANISATION OF DATA SECURITY AND MANAGEMENT OF EMERGENCY SITUATIONS

9. By order the Minister of the Interior shall appoint a data security manager of the Register (hereinafter referred to as the Security Manager) responsible for implementation and control of the Register data security policy.

10. The Security Manager shall submit proposals to the head of the authority managing the Register with regard to the appointment of the Register administrators who would be directly accountable to the Security Manager for the performance of functions assigned thereto.

11. The Register users must have relevant qualification (professional development for information technology users, introductory training for secure data handling, ECDL user certificate, etc.) and experience of work with applications. The Register users must be familiarised with documents regulating data handling.

12. The Security Manager and administrators must have knowledge of basic security policy principles and work with computer networks to ensure security thereof and to have experience of administration and support of Windows, Unix and Oracle systemware tools.

13. The Register users having noticed any violations of the security policy, signs of criminal offences or any data security means not functioning or functioning improperly must immediately inform the administrator performing the relevant function, and in the case of their absence – the Security Manager.

14. In the event of emergency actions of the Register users shall be regulated by the Plan of Emergency Management submitted for approval to the Minister of the Interior by the Security Manager. The main provisions of the Plan shall be as follows: protection of life and health of the Register users, restoration of the Register function and training of the Register users.

IV. RISK ASSESSMENT AND DETAILED WORK PROCEDURE

15. The main risk reduction tools of the Register shall be stipulated in the risk statement approved by the Minister of the Interior and drafted by the Security Manager having assessed risk factors, i.e. subjective non-deliberate factors (data handling errors and mistakes, data deletion, erroneous data provision, physical failure of information technology, software errors, etc.), subjective deliberate factors (unauthorised use of the Register to obtain data, data change or deletion, theft of information technologies, etc.) and force majeure factors (events listed in paragraph 3 of the Rules for Release from Liability in the Case of Force Majeure Circumstances approved by Resolution No. 840 of the Government of the Republic of Lithuania of 15 July 1996 (*Official Gazette*, 1996, No. 68-1652)).

16. When handling the Register data and ensuring security thereof, the following legal acts shall be followed:

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

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

16.3. the Register Regulations;

16.4. the General Data Security Requirements;

16.5. the Lithuanian Standard LST ISO/IEC 17799:2005, Lithuanian and international standards of the group on Information Technology. Security Equipment regulating secure data handling;

16.6. other legal acts regulating legitimacy of data handling, activities of authorities managing the Register and data security management.

17. Specific data handling and protection procedures of the Register shall be described in the detailed Rules for Data Handling submitted for approval to the Minister of the Interior by the Security Manager.

V. RESPONSIBILITY OF THE REGISTER USERS

18. The Register users must ensure security of the Register data and data handled therein.

19. The Register data may be handled only by the Register users having familiarised themselves with the Security Regulations and other legal acts regulating the security policy and having expressed their written consent to observe the requirements of those legal acts.

20. Such familiarisation of the Register users with the Security Regulations and other legal acts regulating the security policy and their responsibility for the failure to follow those requirements shall be organised by the Security Manager to be confirmed by signatures of the Register users. The Register users shall also be informed in writing about any changes to the Security Regulations or invalidation of, amendment to or adoption of other legal acts regulating the security policy.

21. Data security training must continuously be organised for the Register users who must also be reminded of security aspects by various means (e.g. reminders by e-mail, organising topical seminars, memos for new employees, etc.).

22. The Register users having violated the requirements of the Security Regulations or other legal acts regulating the security policy shall be held responsible in accordance with the procedure set out in the laws.

VI. PROCEDURE OF UPDATING THE REGULATIONS

23. The Security Manager seeking to ensure the security of the Register data and data handled therein shall submit proposals to the Minister of the Interior concerning any amendments to the Security Regulations or adoption of, amendment to or invalidation of other legal acts regulating the security policy.

24. The Security Regulations and other legal acts regulating the security policy must be essentially revised when carrying out the audit referred to in paragraph 25 hereof and amended, if need be, at least once a year.

VII. FINAL PROVISIONS

25. To enforce the provisions stipulated herein and in other legal acts regulating the security policy, the Security Manager shall organise the annual audit which shall:

25.1. evaluate the compliance hereof and other legal acts regulating the security policy with the real data security situation;

25.2. perform the stock-taking of all hardware and software of the authority managing the Register;

25.3. check at least 10 percent of computerised workplaces of the Register users, the software installed in all computers and configuration thereof;

25.4. review the conformity of the rights granted to the Register users to their functions accordingly expanding or limiting those functions;

25.5. assess readiness to restore the Register function in the case of emergency.

26. Following the audit, the Plan for Removal of Faults Revealed shall be drafted and submitted for approval to the Minister of the Interior who also appoints persons in charge of implementation and terms of implementation.