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

REGARDING THE DEPARTMENTAL REGISTER OF CRIMINAL ACTS

26 January 2006 No. 1V-36
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 e s t a b l i s h the Departmental Register of Criminal Acts based on the Criminal Statistics central database managed in accordance with the Instructions for Centralised Accounting of Criminal Acts, Persons Having Committed Them and Victims Thereof approved by Order No. IV-160 of the Minister of the Interior of the Republic of Lithuania of 8 May 2003 (*Official Gazette*, 2003, No. 50-2230).

2. I hereby a p p r o v e:

2.1. the Regulations of the Departmental Register of Criminal Acts (attached hereto);

2.2. the Regulations of Data Security of the Departmental Register of Criminal Acts (attached hereto).

3. I hereby e s t a b l i s h that the Departmental Register of Criminal Acts shall come into force on 1 July 2006.

4. I hereby a s s i g n 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 Criminal Acts to draft and submit to the Minister of the Interior:

4.1. the draft amendment to the Instructions for Centralised Accounting of Criminal Acts, Persons Having Committed Them and Victims Thereof;

4.2. draft detailed instructions for handling the data of the Departmental Register of Criminal Acts, procedure descriptions and the Rules for Secure Data Handling.

MINISTER OF THE INTERIOR GINTARAS FURMANAVIČIUS

APPROVED
by Order No. 1V-36 of the Minister of
the Interior of the Republic of Lithuania
of 26 January 2006

REGULATIONS OF THE DEPARTMENTAL REGISTER OF CRIMINAL ACTS

I. GENERAL PROVISIONS

1. The Regulations of the Departmental Register of Criminal Acts (hereinafter referred to as the Regulations) shall regulate the purpose of the Departmental Register of Criminal Acts constituting a part of the information system of the Ministry of the Interior (hereinafter referred to as the Register), the Register objects, institutions managing the Register, the Register data providers, rights and duties thereof, data handling, interaction with other registers, 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 shall be criminal acts (crimes and misdemeanours) provided for in the Criminal Code of the Republic of Lithuania (*Official Gazette*, 2000, No. 89-2741) (hereinafter referred to as the CC).

4. The purpose of handling personal data in the Register shall be investigation and prevention of criminal acts, accounting of suspected (accused) persons and victims and drafting statistical reports about criminal acts, suspected (accused) persons and victims.

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

6. Providers of the Register data shall be the Special Investigation Service of the Republic of Lithuania, the Military Police of the Lithuanian Army, the National Security Department of the Republic of Lithuania, the Customs Department under the Ministry of Finance of the Republic of Lithuania or another customs authority authorised thereby that performs a pre-trial investigation, the Prison Department under the Ministry

of Justice of the Republic of Lithuania, detention facilities, investigatory isolation wards and penitentiary institutions, prosecutor's offices and courts.

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 CC;

7.4. the Code of Criminal Procedure of the Republic of Lithuania (*Official Gazette*, 2002, No. 37-1341) (hereinafter referred to as the CCP);

7.5. 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) (hereinafter referred to as the Instructions);

7.6. the Rules for Forming Key Statistical Indicators of Criminal Acts, Persons Having Committed Them and Victims Thereof approved by Order No. 1V-264 of the Minister of the Interior of the Republic of Lithuania of 30 June 2003;

7.7. the Instructions for Storage, Use and Destruction of Criminal Cases Discontinued and Criminal Cases Where the Pre-Trial Investigation Is Discontinued approved by Order No. 1V-68 of the Minister of the Interior of the Republic of Lithuania of 12 March 2004 (*Official Gazette*, 2004, No. 52-1738);

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

II. AUTHORITIES MANAGING THE REGISTER

8. The Managing Authority managing the Register shall be the Ministry of the Interior of the Republic of Lithuania.

9. Authorities managing the Register:

9.1. 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);

9.2. the Police Department under the Ministry of the Interior of the Republic of Lithuania, specialised and territorial police departments (hereinafter referred to as police departments);

9.3. the Financial Crime Investigation Service under the Ministry of the Interior;

9.4. the Fire and Rescue Department under the Ministry of the Interior;

9.5. the State Border Guard Service under the Ministry of the Interior of the Republic of Lithuania.

10. The Managing Authority managing the Register shall:

10.1. coordinate and ensure proper work of authorities managing the Register and supervise those institutions in due course;

10.2. supervise observance of the Register Data Security Requirements;

10.3. approve legal acts related to the Register management and security of the Register data;

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

10.5. organise and coordinate training of civil servants and employees employed under employment contracts in authorities managing the Register handling the Register data;

10.6. execute agreements on provision of data to the Register stipulating the procedure for provision of the Register data;

10.7. perform other functions stipulated in the Regulations, the Law of the Republic of Lithuania on State Registers and other legal acts.

11. Authorities managing the Register:

11.1. The Information and Communications Department shall:

11.1.1. ensure that the Register would function without interruption, organise and coordinate or perform the works to support and update hardware and software of the Register;

11.1.2. draft legal acts related to the Register data management and security;

11.1.3. consider proposals of other authorities managing the Register regarding improvements of the Register, summarise them and draft legal acts;

11.1.4. accept from the Register data providers listed in paragraph 22 hereof filled-in statistical cards and amendments to data submitted thereby in writing, check correctness of the data provided thereto and register the Register objects by entering the data provided thereto into the Register;

11.1.5. accumulate, process, systemise and store the Register data, update, correct and supplement inaccurate, incomprehensive or incorrect data of the Register and delete illegitimately accumulated data of the Register;

11.1.6. each month within the first 3 working days check the summary data of the Register required for drafting statistical reports on criminal acts, suspected (accused) persons and victims for the reporting month with authorities managing the Register and the Register data providers;

11.1.7. on the grounds of the Register data draft and publish in the Internet official summarised statistical reports about criminal acts, persons suspected (accused) of committing criminal acts and victims of criminal acts registered;

11.1.8. provide data about the Register objects registered thereby and by other authorities managing the Register under data provision agreements and on the grounds of applications of data recipients (in the event of single data provision);

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

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

11.1.11. ensure the interaction of the Register with related registers and information systems;

11.1.12. ensure that the Register would be managed in accordance with the Regulations and other legal acts;

11.1.13. within its competence perform other functions of handling the Register data stipulated in the Regulations and other legal acts.

11.2. Other authorities managing the Register shall:

11.2.1. fill in statistical cards and register the Register objects by entering data of statistical cards into the Register;

11.2.2. accept from the Register data providers filled-in statistical cards and amendments to data submitted thereby in writing, check correctness of the data provided thereto and enter the data provided thereto into the Register;

11.2.3. update and correct incorrect data and supplement inaccurate or incomprehensive data entered into the Register thereby;

11.2.4. submit proposals to the Information and Communications Department with regard to improvement of the Register;

11.2.5. provide only the Register data entered into the Register thereby on the grounds of applications of data recipients;

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

11.2.7. ensure proper functioning of the Register and security of the Register data and documents;

11.2.8. ensure that the Register would be managed in accordance with the Regulations and other legal acts;

11.2.9. within its competence perform other functions of handling the Register data stipulated in the Regulations and other legal acts, except for deletion of the Register data.

12. The Managing Authority managing the Register shall be the manager of personal data of the Register, and authorities managing the Register shall be managers of personal data.

III. REGISTER DATA

13. The following data shall be handled within the Register:

13.1. identification code of the Register object generated by the programme.

13.2. Data of a criminal act:

13.2.1. code of a pre-trial investigation institution or prosecutor's office initiating/finalising the pre-trial investigation or a court having adopted the judgment of conviction in a private accusation case;

13.2.2. number of the criminal case;

13.2.3. number of the criminal act (episode) where several criminal acts are investigated in a pre-trial investigation case;

13.2.4. registration number and date of a complaint, statement, notice or official notice about a criminal act based whereon the pre-trial investigation is initiated;

13.2.5. date of entering data into the Register/sending a card to the Information and Communications Department;

13.2.6. date and time of committing the criminal act;

13.2.7. description of the criminal act;

13.2.8. date of initiating a pre-trial investigation or a private accusation case;

13.2.9. an article, part and paragraph of the CC providing for the criminal act with regard whereto the pre-trial investigation is performed;

13.2.10. stages of committing the criminal act;

13.2.11. the suspect identified/unidentified;

13.2.12. natural or legal persons have suffered or legitimate state interests are violated during the criminal act;

13.2.13. unidentified killed persons (a newborn, a minor, an adult) found;

13.2.14. location of committing the criminal act;

13.2.15. precise place of committing the criminal act;

13.2.16. assassinated object;

13.2.17. ways of committing the criminal act;

13.2.18. tools and means of committing the criminal act;

13.2.19. additional marks on the criminal act committed;

13.2.20. units/services protecting the assassinated object: units of the Ministry of the Interior and of the Ministry of National Defence, security companies, etc.;

13.2.21. protection equipment of the assassinated object activated/not activated, kinds of protection;

13.2.22. number of persons suspected (accused) of committing the criminal act;

13.2.23. the criminal act has been committed by accomplices or an organised group or a criminal alliance;

13.2.24. natural or legal person suspected (accused) of committing the criminal act;

13.2.25. name and surname of the prosecutor or judge having adopted a decision to discontinue or resume the pre-trial investigation, name of the prosecutor's office or court having made the decision, an article, part and paragraph of the CCP specifying the kind of the decision made, date of the decision;

13.2.26. the pre-trial investigation has been carried out by: a prosecutor, a pre-trial investigation officer or a judge having scrutinised the private accusation case;

13.2.27. motive for committing the criminal act;

13.2.28. the degree of material damage established during the pre-trial investigation (amount in LTL);

13.2.29. property, cash, securities and foreign currency seized (found) during the pre-trial investigation (amount in LTL);

13.2.30. precious (non-precious) metals, radioactive and poisonous substances seized (found) during the pre-trial investigation (in grams);

13.2.31. drugs and psychotropic substances or precursors thereof seized (found) during the pre-trial investigation (in mg, g, ml and pcs.);

13.2.32. fake money seized (withdrawn from circulation) during the pre-trial investigation (in units);

13.2.33. weapons or other accoutrements seized (found) during the pre-trial investigation (in units);

13.2.34. the suspect has been identified with the help of the pre-trial investigation officer, the prosecutor, the public, the victim or other persons;

13.2.35. scientific and technical tools has been used when detecting the criminal act;

13.2.36. detection (prevention) of the criminal act based on a notice or operational case;

13.2.37. kinds of administrative sanctions imposed on the suspected (accused) person prior to drafting the indictment or discontinuation of the criminal proceedings: warning, fine, administrative arrest, etc.;

13.2.38. kinds of measures of restraint imposed on the suspected (accused) person;

13.2.39. conditions of release from criminal liability applicable to the suspected (accused) person prior to drafting the indictment or discontinuation of the criminal proceedings: released from criminal liability where the criminal act loses its degree of danger, for low significance of the criminal act, for extenuating circumstances, etc.;

13.2.40. number of the criminal case wherewith the criminal case with regard to which the pre-trial investigation is initiated is linked (wherefrom it is isolated);

13.2.41. date of transfer of the criminal case to the prosecutor to make a decision to finish the pre-trial investigation;
13.2.42. the person has suffered from their spouse, co-habitant, father, mother, etc.;
13.2.43. circumstances of committing the criminal act from which the person has suffered;
13.2.44. the natural person having suffered during the criminal act: killed, injured;
13.2.45. the victim has suffered material damage, physical violence, sexual violence, psychological violence or neglect.
13.3. Data of the natural and legal person suspected (accused):
13.3.1. personal code of the natural person;
13.3.2. name (names);
13.3.3. surname (surnames);
13.3.4. date of birth of a foreigner or a person without citizenship;
13.3.5. age of the person at the moment of committing the criminal act;
13.3.6. sex;
13.3.7. citizenship;
13.3.8. nationality;
13.3.9. education;
13.3.10. employment: employed, student, unemployed, etc.;
13.3.11. other signs of the natural person suspected (accused) of committing the criminal act: drug user, recidivist, committed the criminal act whereof the person is suspected (accused) while intoxicated, etc.;
13.3.12. legal person code;
13.3.13. name of the legal person.
13.4. Data of the natural and legal person who is the victim:
13.4.1. personal code of the natural person;
13.4.2. name (names);
13.4.3. surname (surnames);
13.4.4. sex;
13.4.5. age of the person at the moment of committing the criminal act;
13.4.6. date of birth of a foreigner or a person without citizenship;
13.4.7. citizenship;
13.4.8. nationality (collected for statistical purposes only in the form that would not allow directly or indirectly identifying the data subject, except for the cases stipulated in the laws);
13.4.9. education;
13.4.10. employment;
13.4.11. family members with whom the minor victim lives: with parents, with one of the parents, with a relative, with a custodian (carer);
13.4.12. legal person code;
13.4.13. name of the legal person.
13.5. Data of the officer of the pre-trial investigation institution or the prosecutor initiating/finalising the pre-trial investigation or the judge having adopted the judgment of conviction in a private accusation case:
13.5.1. position;
13.5.2. name;
13.5.3. surname.
13.6. Data of criminal cases discontinued and criminal cases where the pre-trial investigation is discontinued:
13.6.1. case accounting number;
13.6.2. period of storing the case;
13.6.3. date until when the case is to be stored;
13.6.4. number and date of the act of the case destruction;
13.6.5. number and date of the decision to continue storing the case;
13.6.6. date until when the period of storing the case is extended.
14. The following classifiers shall be used and handled within the Register:
14.1. codes of pre-trial investigation institutions (Annex 6 to the Instructions);
14.2. codes of prosecutor’s offices (Annex 10 to the Instructions);
14.3. codes of courts (Annex 7 to the Instructions);

14.4. classifier of countries and areas of the world.

IV. REGISTRATION OF THE REGISTER OBJECTS

15. The Register objects shall be registered in accordance with the procedure laid down in the Instructions for Statistical and Accounting Cards Filled In and Submitted to Authorities Managing the Register, the Instructions for Storage, Use and Destruction of Criminal Cases Discontinued and Criminal Cases Where the Pre-Trial Investigation Is Discontinued and the Regulations.

16. Data about the Register objects shall be entered into the Register from the following cards:

16.1. Statistical Card of the criminal act (Annex 1 to the Instructions);

16.2. Statistical Card of the investigation findings (Annex 2 to the Instructions);

16.3. Statistical Card of the person suspected (accused) of committing the criminal act (Annex 3 to the Instructions);

16.4. Statistical Card of decisions made in the criminal case (Annex 4 to the Instructions);

16.5. Statistical Card of the natural or legal person who is the victim (Annex 5 to the Instructions);

16.6. Accounting Card of the criminal case where the pre-trial investigation is discontinued (Annex 3 to the Instructions for Storage, Use and Destruction of Criminal Cases Discontinued and Criminal Cases Where the Pre-Trial Investigation Is Discontinued).

17. The Register data providers shall:

17.1. be responsible for correctness of data contained in cards submitted to authorities managing the Register;

17.2. be obliged within the terms set out herein to submit statistical cards needed for entering the Register object to the authority managing the Register;

17.3. be obliged within 3 working days following the day of change in the Register data to inform the authority managing the Register in writing;

17.4. having submitted a written application be entitled to familiarise themselves with the data submitted thereby and handled within the Register and entered into the Register;

17.5. be entitled to demand in writing to correct incorrect or specify inaccurate or incomprehensive data.

18. The Register data provider having submitted fake statistical cards, having submitted statistical cards late or otherwise failing to meet the requirements of the Regulations and legal acts regulating the Register management shall be held legally liable.

19. Police departments, the Financial Crime Investigation Service under the Ministry of the Interior, the Fire and Rescue Department under the Ministry of the Interior and the State Border Guard Service under the Ministry of the Interior of the Republic of Lithuania shall assign a unique number of the criminal case to every pre-trial investigation initiated, immediately fill in relevant statistical cards specified in paragraphs 16.1-16.5 hereof in accordance with the procedure laid down in the Instructions and immediately enter the data of the statistical cards about the Register objects into the Register database. The case number shall later be used to find data about the Register objects in the Register. This number shall not be changed and may not be used for registering other criminal cases.

20. Police departments, the Financial Crime Investigation Service under the Ministry of the Interior, the Fire and Rescue Department under the Ministry of the Interior and the State Border Guard Service under the Ministry of the Interior of the Republic of Lithuania shall fill in the accounting card referred to in paragraph 16.6 hereof for criminal cases where the pre-trial investigation is discontinued and assign to it a unique case accounting number in accordance with the procedure laid down in the Instructions for Storage, Use and Destruction of Criminal Cases Discontinued and Criminal Cases Where the Pre-Trial Investigation Is Discontinued and enter the data of the accounting card into the Register database.

21. District and circuit prosecutor's offices where they carry out the entire pre-trial investigation with regard to the criminal act committed shall assign a unique number of the criminal case to every pre-trial investigation initiated and immediately fill in relevant statistical cards specified in paragraphs 16.1-16.5 hereof in accordance with the procedure laid down in the Instructions. Within 3 working days following the commencement of the pre-trial investigation district and region circuit prosecutor's offices shall transfer statistical cards to police departments within whose territory the criminal act is committed so that they would enter the data of the statistical cards about the Register objects into the Register database. Within 3 working days following the commencement of the pre-trial investigation city circuit prosecutor's offices shall transfer

statistical cards to chief police commissariats of the city so that they would enter the data of the statistical cards about the Register objects into the Register database.

22. The Customs Department under the Ministry of Finance of the Republic of Lithuania or another customs authority authorised thereby performing the pre-trial investigation, the Special Investigation Service of the Republic of Lithuania, the National Security Department of the Republic of Lithuania, the Military Police of the Lithuanian Army, the Prosecutor's General Office of the Republic of Lithuania where it carries out the entire pre-trial investigation with regard to the criminal act committed, the Prison Department under the Ministry of Justice of the Republic of Lithuania, detention facilities, investigatory isolation wards and penitentiary institutions shall assign a unique number of the criminal case to every pre-trial investigation initiated, immediately fill in relevant statistical cards specified in paragraphs 16.1-16.5 hereof in accordance with the procedure laid down in the Instructions and within 3 working days following the commencement of the pre-trial investigation submit the statistical cards to the Information and Communications Department so that it would enter the data of the statistical cards about the Register objects into the Register database.

23. Courts having scrutinised private accusation cases and made judgments of conviction therein shall fill in statistical cards specified in paragraphs 16.1-16.3 and 16.5 hereof in and within 3 working days following the adoption of the judgment of conviction transfer them to territorial police departments within whose territory the criminal act is committed so that they would assign to it a unique number of the private accusation case in accordance with the procedure laid down in the Instructions and enter the data of the statistical cards about the Register objects into the Register database.

24. The Register objects shall be registered when data thereof is entered into the Register database.

25. When entering data of statistical cards about the Register objects into the Register database, the authority managing the Register shall automatically check data against data of related state and departmental registers. Having established any lack of correspondence between the data received from a related register and the data submitted by the Register data provider, the authority managing the Register must immediately 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 and explanations of circumstances to the authority managing the Register. Only having established inaccuracy of data of a related register or after the data provider specifies this data, the authority managing the Register shall enter the data provided into the Register database.

26. Having established that the statistical cards submitted contain incorrect, incomprehensive and inaccurate data, within 3 working days following the date of becoming aware of the inaccuracies in the data the authority managing the Register shall inform the Register data provider accordingly in writing and return the statistical cards. The provider of the Register data shall be obliged within 5 working days following the receipt of the statistical cards to submit corrected and supplemented statistical cards to the authority managing the Register.

27. Having established that incorrect, inaccurate or incomprehensive data of statistical cards about the Register objects has been entered into the Register database, no later than within 3 working days the authority managing the Register must correct the data and free of charge inform all recipients of the Register data in writing that incorrect, inaccurate and incomprehensive data has been provided to them.

28. A natural person whose data is entered into the Register subject to presenting their personal identification document or a legal person whose data is entered into the Register subject to filing a written application to the Information and Communications Department shall be entitled to familiarise themselves with their data handled within the Register. This right may be restricted in the cases listed in Article 17(2) of the Law of the Republic of Lithuania on Legal Protection of Personal Data. The Information and Communications Department shall present information about personal data handled within the Register in writing within 10 working days following the day of address by the person.

29. The person whose data is entered into the Register and having familiarised themselves with their data handled within the Register shall be entitled to demand that incorrect or inaccurate data would be corrected, incomprehensive data would be supplemented and irrelevant or illegitimately collected data would be deleted. The Information and Communications Department shall be obliged within 5 working days following the receipt of the request and documents certifying the facts specified therein to correct the inaccuracies pointed out and inform in writing the person having submitted the request.

30. The Register data shall be accumulated in the Register database until the end of the current calendar year after which it shall be transferred to the Register database archive where it shall be stored for 75 years following the end of the calendar year when the data is entered into the Register. Statistical cards shall be

stored in accordance with the procedure laid down in the Instructions. Upon expiry of the period of storage of the Register data set, the Register data and documents shall be destroyed in due course.

31. Performing technical and logical control of data, authorities managing the Register shall ensure that when managing the Register no incorrect, inaccurate or incomprehensive data would be entered and that the Register data would correspond to the data of statistical cards submitted for registration.

32. Civil servants and employees working under employment contracts who handle the Register data must sign commitments to keep data a secret in accordance with the procedure laid down in the legal acts.

V. INTERACTION WITH OTHER REGISTERS

33. The Register shall be linked to the Register of Residents of the Republic of Lithuania, the Register of Legal Persons and the Register of Police-Registered Events.

34. Data specified in paragraphs 13.3.1-13.3.3, 13.3.6, 13.3.7, 13.4.1-13.4.3, 13.4.4 and 13.4.7 hereof shall automatically be obtained from the database of the Register of Residents of the Republic of Lithuania.

35. Data specified in paragraphs 13.3.12, 13.3.13, 13.4.12 and 13.4.13 hereof shall automatically be obtained from the database of the Register of Legal Persons.

36. Data specified in paragraphs 13.2.4, 13.2.6, 13.2.7, 13.2.9, 13.2.15-13.2.18 and 13.5 hereof shall automatically be obtained from the database of the Register of Police-Registered Events.

37. Interaction with related registers shall be validated subject to an agreement on data provision.

38. Having detected inaccuracies in data received from a related register, the authority managing the Register shall immediately transfer incorrect, incomprehensive or inaccurate data and explanations of circumstances to the authority managing such a related register.

39. 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 Register data provider for correcting inaccuracies, this term shall be extended up to 7 calendar days. Having corrected the inaccurate data of the Register, the authority managing the Register shall immediately 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

40. The Register data shall be provided in accordance with the procedure laid down in the Law of the Republic of Lithuania on Legal Protection of Personal Data and other legal acts to legal and natural persons subject to a written data recipient's application specifying the purpose of data use or on the grounds of data provision agreements between the data recipient and the Managing Authority managing the Register specifying the purpose, conditions and procedure of use of the data. The Register data recipients may not use the data obtained in any other way or use it for any other purpose than the one set in the data provision agreement or application. The Register data shall be provided to the Register data recipients only to the extent necessary for the purpose for which the data is provided.

41. Ways of providing the Register:

41.1. transferred automatically;

41.2. issuing certificates or other documents;

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

41.4. by other statutory means.

42. The way to provide the Register data shall be coordinated with the Register data recipients and may be changed only subject mutual agreement between the Register data recipient and the authority managing the Register. As requested by the Register data recipient the Register data may be selected and grouped according to the enquiry made by the Register data recipient and provided in the form of extracts or reports in the form provided by the data recipient.

43. Having noticed that data transmitted is inaccurate, recipients of the Register data shall immediately inform the authority managing the Register thereof verbally, in writing, by e-mail or using other means of communication.

44. 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 verbally, in writing, by e-mail or other means of communication and where the information is not confirmed – inform the recipient of the Register data having provided information about the refusal to correct inaccuracies verbally, in writing, by-email or other means of communication.

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

45.1. to natural and legal persons – (about their data handled within the Register) once per calendar year;

45.2 to related registers – subject to agreements on data provision;

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

45.4. to units of the administration of the Ministry of the Interior of the Republic of Lithuania and institutions under the Ministry of the Interior of the Republic of Lithuania – for performance of their direct functions;

45.5. to the Register data providers – only data provided thereby and entered into the Register.

46. The Register data shall be provided to other persons legally entitled to receive the Register data and not listed in paragraph 45 hereof for a fee the size whereof shall be calculated in accordance with the procedure laid down in the legal acts.

47. Official statistical summary reports shall be drafted and published in the Internet based on the Register data.

VII. TRANSMISSION OF THE REGISTER DATA TO FOREIGN COUNTRIES

48. 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.

49. The Register data shall be provided to legal and natural persons of foreign countries non-Member States of the European Union in accordance with the laws and other legal acts of the Republic of Lithuania and international treaties.

VIII. PROTECTION OF THE REGISTER DATA

50. The Information and Communications Department shall be responsible for security of the Register data.

51. Authorities managing the Register shall be responsible for security of data of statistical cards submitted thereto and the Register data handled thereby.

52. The Information and Communications Department shall register the Register data recipients and civil servants and employees working under employment contracts who handle the Register data and work for authorities managing the Register and grant rights to handle the Register data in accordance with the procedure laid down by the Minister of the Interior.

53. When managing the Register, software and hardware tools for data security must be provided together with room security and administrative means intended to ensure accuracy of the Register data and to protect it from accidental or unauthorised deletion, modification, use, disclosure and any other unauthorised act therewith. The above means and tools must ensure the security level matching the nature of the Register data to be protected and the risk of handling it. These means and tools, the security requirements of the Register data and implementation thereof shall be 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.

54. Security of the Register shall be ensured by 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) and other legal acts regulating security of the Register data.

IX. REGISTER FUNDING

55. 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

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

57. 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 Finance of the Republic of Lithuania
Zigmantas Balčytis
13 October 2005

COORDINATED
Minister of Justice of the Republic of Lithuania
Gintautas Bužinskas
21 October 2005

COORDINATED
Minister of National Defence of the Republic of Lithuania
Gediminas Kirkilas
3 October 2005

COORDINATED
Director of the National Court Administration
of the Republic of Lithuania
Raimondas Bakšys
30 September 2005

COORDINATED
Prosecutor General ad interim
of the Republic of Lithuania
Vytautas Barkauskas
30 September 2005

COORDINATED
Director of the Special Investigation Service
of the Republic of Lithuania
Povilas Malakauskas
4 October 2005

COORDINATED
Director General of the National Security
Department of the Republic of Lithuania
Arvydas Pocius
4 October 2005

APPROVED
by Order No. 1V-36 of the Minister of
the Interior of the Republic of Lithuania
of 26 January 2006

SECURITY REGULATIONS OF THE DEPARTMENTAL REGISTER OF CRIMINAL ACTS

I. GENERAL PROVISIONS

1. The purpose of the Regulations of the Data Security of the Departmental Register of Criminal Acts (hereinafter referred to as the Regulations) shall be to create conditions for secure automated handling of the data of the Departmental Register of Criminal Acts (hereinafter referred to as the Register).

2. The Regulations shall regulate 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 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 perform actions of handling the Register data.

5. Objects of the Register shall be criminal acts (crimes and misdemeanours) provided for in the Criminal Code of the Republic of Lithuania (*Official Gazette*, 2000, No. 89-2741).

6. 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.

7. The Register shall handle the following data groups provided for in the Register Regulations:

7.1. identification code of the Register object generated by the programme;

7.2. data of a criminal act;

7.3. data of the natural and legal person suspected (accused);

7.4. data of the natural and legal person who is the victim;

7.5. data of the officer of the pre-trial investigation institution or the prosecutor initiating/finalising the pre-trial investigation or the judge having adopted the judgment of conviction in a private accusation case;

7.6. data of criminal cases discontinued and criminal cases where the pre-trial investigation is discontinued;

7.7. classifiers used and handled within the Register.

III. ORGANISATION OF DATA SECURITY AND MANAGEMENT OF EMERGENCY SITUATIONS

8. 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.

9. 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.

10. The Register users must have relevant qualification (professional development for information technology users, general computer literacy ECDL user certificate, etc.) and experience of work with applications. The Register users must be trained to securely handle the Register data, i.e. an introductory

training to security handle data must organised and users must be familiarised with documents regulating data handling.

11. 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.

12. The Register users having noticed any violations of the security policy, signs of misdemeanours 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.

13. 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

14. 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 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)).

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

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

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

15.3. the Register Regulations;

15.4. the General Data Security Requirements;

15.5. the Lithuanian Standard LST ISO/IEC 17799:2002, Lithuanian and international standards of the group on Information Technology. Security Equipment regulating secure data handling.

16. 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

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

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

19. Such familiarisation of the Register users with the 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. Users shall also be informed in writing about any changes to the Regulations or invalidation of, amendment to or adoption of other legal acts regulating the security policy.

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

21. The Register users having violated the requirements of the 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

22. 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 Regulations or adoption of, amendment to or invalidation of other legal acts regulating the security policy.

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

VII. FINAL PROVISIONS

24. 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:

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

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

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

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

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

25. 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.

_____