
NB: Unofficial translation

Act on the Processing of Personal Data by the Police
(761/2003)

Chapter 1
General provisions

Section 1
Scope of the Act

(1) This Act applies to the automatic and other processing of personal data needed for the performance of duties as referred to in section 1 of the Police Act (493/1995), where the personal data constitutes or is intended to constitute a personal data file or part thereof. The Personal Data Act (523/1999) and the Act on the Openness of Government Activities (621/1999) apply to the processing of personal data, unless otherwise provided in this or any other Act.

(2) In addition to what is provided in this Act, international agreements binding on Finland shall also be observed.

Chapter 2
Police information systems

Section 2
Data System for Police Matters

(1) The Data System for Police Matters is a permanent, computerized personal data file intended for nationwide use by the police. The Data System for Police Matters may contain personal data whose processing is necessary for the performance of duties laid down in section 1(1) of the Police Act.

(2) The data that may be recorded in the data system on the identity of persons suspected of an offence or subject to a pre-trial investigation, police investigation, police action or coercive measure consists of the person's full name, date of birth, personal identity code, sex, mother tongue, nationality, marital status, country of birth, municipality of residence at birth, municipality of residence, occupation, address and telephone number or other contact details, information on the person's death, travel document information in the case of an alien, and any personal data relevant to the person's own safety or the occupational safety of the police.

(3) In addition, other necessary data obtained for the performance of duties laid down in section 1(1) of the Police Act may be recorded in the data system, as follows:

1) in the case of persons for whom an apprehension warrant has been issued, persons subject to a prohibition on engaging in business, restraining order or travel ban, persons who have been granted a conditional discharge, persons protected by a restraining order and persons under surveillance, in order to find, monitor, conduct surveillance on or protect such persons, information on the reasons for action taken, the requested action, the warrant-issuing authority, the expiry of the warrant, and other information needed to monitor warrants of apprehension, (*apprehension warrant data*);

2) in the case of vehicles and number plates that have been stolen or that are searched for some other reason, identification data in order to recover such property and information needed to return the property to its owner or holder, and, in the case of searched persons or persons under surveillance who are travelling in motor vehicles, information needed to find such persons (*searched motor vehicle data*);

3) in the case of property that has been lost through crime or taken possession of by the police or that is missing or held by a missing person, identification data in order to recover such property, information needed to return the property to its owner or holder, and information needed to solve missing persons cases (*property data*);

4) in the case of persons apprehended, arrested or detained under the Pre-trial Investigation Act (449/1987), the Coercive Measures Act (450/1987), the Police Act or some other statute, in order to monitor and supervise periods of deprivation of liberty and to ensure safety in custody, the information on arrest referred to in section 22 of the Pre-trial Investigation and Coercive Measures Decree (575/1988), and information concerning reports of offences and apprehension, and, in individual cases, information relevant to safety in custody concerning persons who have been deprived of their liberty (*arrested persons data*);

5) in the case of persons suspected of an offence, for the purpose of a unified search for recorded reports of offences, the reference number of the report of an offence, the date and place of the offence, the designation of the offence, the statute of limitations for the offence, and the penalties and other sanctions imposed for the offence (*crime report index and sanctions data*);

6) information recorded by the police that, for reasons of urgency, danger, crime prevention or criminal investigation, particularly needs to be communicated to bring it to the attention of police units and to focus supervision (*message transmission data*);

7) in the case of suspected offences, in order to classify and analyse criminal modus operandi, information notified in reports of offences and entered in pre-trial investigation records, information on the injured party and the suspect, information identifying the offence and concerning the description of events, information on criminal property, information describing the classification of the offender, the case or the act, and information needed for the linking of offences and for a forensic investigation (*modus operandi data*);

8) in the case of persons reported missing, information needed to find such persons and, in the case of unidentified deceased persons, information needed to identify such persons (*identification data*);

9) in the case of persons suspected or convicted of an offence, for the purpose of identifying persons suspected of an offence, investigating offences and registering offenders, the personal descriptions laid down in Chapter 6, section 4(1) and (4) of the Coercive Measures Act, and the DNA profiles laid down in section 5 of the same Chapter, the video images and shoeprints of the person, information on the suspected offence, and information concerning registration and the classification of the person (*personal description data*);

10) information obtained, for the purpose of conducting and keeping a record of investigation and executive assistance duties, in a pre-trial investigation as referred to in the Pre-trial Investigation Act, in a police investigation as referred to in the Police Act, in connection with police action or executive assistance duties, or in connection with the application of the Coercive Measures Act (*investigation and executive assistance data*), as follows:

a) on persons suspected of the offence, persons reporting the offence, witnesses, injured parties, and persons otherwise connected with the report of an offence;

b) on the designations in reports of offences and in other reports, and on coercive measures, police action and the stages of pre-trial and police investigations;

c) on other necessary descriptions, circumstances and particulars concerning a police duty, police action or an event;

11) in the case of investigation and executive assistance data, for the purpose of a document search from the police archive, the identification data concerning the report and the case, and a summary of the statement section (*investigation and executive assistance archive data*).

Section 3

Data System for Administrative Matters

(1) The Data System for Administrative Matters is a permanent, computerized personal data file intended for nationwide use by the police. The Data System for Administrative Matters may contain personal data whose processing is necessary for the performance of duties laid down in section 1(3) of the Police Act.

(2) The data that may be recorded in the data system on the identity of persons consists of the full name, date of birth, personal identity code, sex, mother tongue, nationality, marital status, country of birth, municipality of residence at birth, municipality of residence, occupation, address and telephone number or other contact details, information on the person's death, and travel document information in the case of an alien.

(3) In addition, other necessary data obtained for the performance of duties as referred to in section 1(3) of the Police Act may be recorded in the data system, as follows:

1) information on the applications, permits and licences, police action, decisions, obstacles, reprimands, notifications and examinations referred to in the Firearms Act (1/1998) that is necessary for the performance of police duties laid down in the Firearms Act (*data on firearms permits and licences*);

2) information on the applications, decisions, authorizations, police action, obstacles, reprimands and notifications referred to in the Identity Card Act (829/1999) that is necessary for the performance of police duties laid down in the Identity Card Act, and, for the performance of police duties laid down in the Passport Act (642/1986), information on passport applications and decisions on passport matters, passports or other travel documents issued by the Finnish authorities, passports that have been lost, stolen or taken into possession, and on obstacles to issuing a passport and reprimands concerning passport matters (*identity card and passport data*);

3) a personal photograph and specimen signature, for the purpose of identifying persons and preparing documents indicating identity, given by the person to the police or to the authorities of the foreign affairs

administration when applying for an authorization or decision for which a personal photograph and specimen signature are needed; a personal photograph and specimen signature recorded as image data may, with the consent of the person concerned, be used in the preparation of any other administrative authorization or decision applied for by the person besides the document for which the personal photograph and specimen signature were submitted (*image data*);

4) information, for the purposes laid down in Chapter 4 of the Act on Background Checks (177/2002), confirming that the person has been subject to a limited background check as referred to in the Act, and the time at which the background check was made, and other information needed to identify the background check (*local police background check data*);

5) information on the applications, decisions, cards, police action, obstacles, reprimands, notifications and inspections referred to in the Private Security Services Act (282/2002) and in further provisions issued under it, and on the applications, decisions, authorizations, cards, police action, obstacles, reprimands and notifications referred to in the Security Stewards Act (533/1999) and in provisions issued under it that is necessary for the performance of police duties laid down in the Private Security Services Act and the Security Stewards Act (*security sector supervision data*);

6) in the case of aliens as referred to in section 53a of the Aliens Act (378/1991), for the performance of duties laid down in the same section, the personal descriptions referred to in the section, and travel document information (*aliens identification data*).

Section 4
Suspect Data System

(1) The Suspect Data System is a permanent, computerized personal data file intended for nationwide use by the police.

(2) The Suspect Data System may contain criminal intelligence, surveillance and observation data, obtained for the performance of

duties laid down in section 1(1) of the Police Act, on persons who are, with reason, suspected of:

1) being guilty of or having been guilty of an offence subject to imprisonment; or

2) contributing to or having contributed to an offence subject to imprisonment of more than six months, or to an unlawful use of narcotics.

(3) The data that may be recorded in the data system on the identity of persons consists of the full name, date of birth, personal identity code, sex, mother tongue, nationality, marital status, country of birth, municipality of residence at birth, municipality of residence, occupation, address and telephone number or other contact details, information on the person's death, and travel document information in the case of an alien.

(4) The Suspect Data System may only be used with the aid of a technical interface by police personnel appointed to criminal intelligence and surveillance duties.

Section 5
Operational Data System of the Security Police

(1) The Operational Data System of the Security Police is a permanent, computerized personal data file intended for use by the Security Police.

(2) The Operational Data System of the Security Police may contain information that needs to be processed to prevent or investigate plans or offences that endanger judicial or social order or State security.

(3) The data that may be recorded in the data system on the identity of persons consists of the full name, date of birth, personal identity code, sex, mother tongue, nationality, marital status, country of birth, municipality of residence at birth, municipality of residence, occupation, address and telephone number or other contact details,

information on the person’s death, and travel document information in the case of an alien.

(4) Information on basic background checks and extended background checks conducted by the Security Police as referred to in the Act on Background Checks, identification data on persons subject to the background checks and the time at which the background checks were made are also recorded in the Operational Data System of the Security Police.

Section 6

Other personal data files kept by the police

(1) In addition to the permanent, computerized, nationwide information systems referred to in sections 2-4 and in sections 30 and 31, the police may also keep temporary or manually maintained personal data files for nationwide use.

(2) With the exception of the information systems referred to in sections 2-5 and in sections 30 and 31, a police personal data file may also be established:

1) for use by more than one police unit; or

2) for use by a police unit.

(3) Information necessary for the performance of duties laid down in section 1(1) of the Police Act may only be collected and recorded in police personal data files established for the purpose of performing the duties in question. Information necessary for the performance of duties laid down in section 1(3) of the Police Act may only be recorded in police personal data files established for the purpose of performing the duties in question.

Section 7

File keepers

The file keeper of the personal data files referred to in sections 2-4 and 6(1) and in sections 30 and 31 is the Supreme Police Command; the file keeper of the personal data file referred to in section 5 is the Security Police; and the file keeper of the personal data file referred to in section 6(2) is the police unit in charge of the operation.

Section 8

Establishing personal data files

(1) The decision to establish a personal data file as referred to in section 6(1) is made by the Supreme Police Command, and the decision to establish a personal data file as referred to in section 6(2) is made by the police unit in charge of the operation.

(2) Establishing personal data files other than those referred to in sections 2-5 and in sections 30 and 31 requires a decision in writing. In respect of temporary or manually maintained personal data files for nationwide use as referred to in section 6, the decision on establishing a file and any significant alteration to it shall be notified to the Data Protection Ombudsman no later than one month before the file is established or altered. The decision to establish a personal data file shall state the purpose of use of the file.

Section 9

Emergency response centre data system and Register of Aliens

(1) Provisions on the emergency response centre data system are laid down in the Emergency Response Centres Act (157/2000) and provisions on the Register of Aliens in the Act on the Register of Aliens (1270/1997).

Chapter 3
Special provisions on processing personal data

Section 10

Processing sensitive data

(1) The data referred to in section 11(1)(3) of the Personal Data Act may be collected and recorded in a police personal data file and otherwise processed if the data is necessary for the purpose of use of the file.

(2) The data referred to in section 11(1)(1-2) and 11(1)(4-6) of the Personal Data Act may only be collected and recorded in a police personal data file or otherwise processed if this is essential for the performance of an individual police duty. The data referred to in section 11(1)(4) may also be collected and recorded in a police personal data file and otherwise processed if this is essential to ensure the personal safety of the data subject or the occupational safety of the police.

(3) The data referred to in section 11(1)(1-2) and 11(1)(4-6) of the Personal Data Act may not, however, be collected and recorded in the personal data file referred to in section 31.

(4) Provisions on restrictions concerning the recording of DNA profiles are laid down in Chapter 6, section 5 of the Coercive Measures Act.

Section 11

Information obtained through interception

(1) If information obtained through the interception referred to in the Police Act concerns an offence other than the one whose prevention or discontinuation was the purpose of the interception, the information may not be recorded in a personal data file, unless it concerns an offence for which interception could be conducted in order to prevent or discontinue it.

(2) Provisions on recording in a personal data file information obtained through the telecommunications interception or interception referred to in the Coercive Measures Act are laid down in the Coercive Measures Act.

Section 12

Processing information not related to an individual duty

(1) Information necessary for the performance of duties laid down in section 1(1) of the Police Act which was obtained when carrying out an individual police duty but which is not related to the duty in question or to another duty already being conducted may only be collected and recorded in the personal data files referred to in sections 4, 5, 30 and 31 or in a temporary personal data file as referred to in section 6(2)(2) for recording purposes laid down in the sections in question.

(2) When recording information, an assessment of the reliability of the information provider and the accuracy of the information shall be attached with it, where possible.

Section 13

Police access to information from certain registers

(1) In addition to what is provided in the Police Act or in any other Act, the police have the right to obtain, for performing their duties and maintaining their personal data files, information from registers, as laid down in subsection 2.

(2) Notwithstanding any secrecy provisions, the police have the right, in the manner agreed with the relevant file keeper, and with the aid of a technical interface or in machine-readable form, to obtain:

1) data from the Finnish Vehicle Administration’s data system of road traffic on vehicles searched by the police or on vehicles subject to a pre-trial investigation, police investigation or other investigation;

2) data from the State Provincial Offices’ traffic licence control systems needed for the surveillance of authorized traffic, and data from the local Register Offices’ boat registers needed in boat traffic surveillance;

3) data from the judicial administration’s information systems on criminal matters that are or have been subject to consideration of charges, decisions of prosecutors, criminal matters that are or have been pending in court, final court decisions, and on persons for whom

the judicial administration authorities have issued an apprehension warrant, data from the Legal Register Centre's information system on the enforcement of fines, and data from the information systems of the Probation Service and the Prison Service on persons undergoing or having undergone punishment involving deprivation of liberty; provisions on obtaining data from the criminal records are, however, laid down in the Criminal Records Act (770/1993);

4) notifications and notices concerning private entrepreneurs from the Trade Register kept by the National Board of Patents and Registration of Finland;

5) information from telecommunications operators, as laid down in Chapter 5a, section 3 of the Coercive Measures Act, section 31c of the Police Act and sections 35 and 36 of the Act on Data Protection in Electronic Communications (516/2004); (523/2004)

6) data from the information systems of the Ministry for Foreign Affairs on decisions concerning passports, visas and residence and work permits;

7) data from the Directorate of Immigration's information systems that is necessary for processing matters as referred to in the Aliens Act and for monitoring compliance with the Aliens Act;

8) data from the Population Register Centre's population information system, as laid down in sections 4 and 5 of the Population Information Act (507/1993).

(3) Before data is supplied to the police with the aid of a technical interface, the police shall present an account of data security in the manner referred to in section 32(1) of the Personal Data Act.

Section 14

Supplying information from other authorities to the police online or in machine-readable form for the purpose of recording

(1) In a manner agreed with the file keeper, police personal data files may be supplied with information online or in machine-readable form for the purpose of recording, as follows:

1) the judicial administration authorities, the Probation Service and the Prison Service and the Legal Register Centre may supply information on persons for whom they have issued an apprehension warrant, and the Prison Service on the personal descriptions of persons undergoing or having undergone punishment involving deprivation of liberty;

2) the Frontier Guard, the Customs and the military authorities may supply information on persons for whom they have issued an apprehension warrant, on aliens, on the identity of persons, on the personal descriptions of aliens, and information necessary for preventing and investigating offences falling within the jurisdiction of the Frontier Guard and the Customs;

3) the foreign affairs administration authorities may supply information on passport and visa decisions and on residence and work permit decisions.

Chapter 4
Utilizing and supplying data

Section 15
Utilizing data for a purpose equivalent to data collection and recording

(1) Personal data files established for nationwide use by the police are available to all police units with the exception of the Police College of Finland, the National Police School of Finland, the Police IT Management Agency and the Police Technical Centre. Personal data files as referred to in section 6(2) established for more restricted use than nationwide use are only available to those police units for whose use they were established.

(2) The police have the right to utilize data from a personal data file established for the purpose of performing duties laid down in section

1(1) of the Police Act if the data is necessary for the performance of the duties in question. The police have the right to utilize data from a personal data file established for the purpose of performing duties laid down in section 1(3) of the Police Act if the data is necessary for the performance of the duty for which the data was collected and recorded.

Section 16

Utilizing data for a purpose other than one equivalent to data collection and recording

(1) The police have the right, unless otherwise provided below, to utilize data from a police personal data file for a purpose other than one equivalent to data collection and recording if the data is necessary:

1) for ensuring State security;

2) for countering an immediate danger threatening life or health or for preventing significant damage to property;

3) for preventing or investigating an offence subject to imprisonment;

4) for establishing a person’s identity when undertaking an individual police duty that necessarily requires verification of identity;

5) when deciding or issuing an opinion on the granting or validity of an authorization if it has been laid down that a requirement for the granting or validity of the authorization is the applicant’s or holder’s reliability, suitability or other such attribute whose assessment requires information on the state of health, intoxicant use, criminal guilt or violent behaviour of the applicant or holder.

(2) Data from a police personal data file may also be used in police research and planning work. Such data may similarly be used in police training activities if the data is essential for carrying out the training.

(3) Data from the Suspect Data System referred to in section 4 may not be used for the performance of the duties referred to in subsection 1(5).

Section 17

Supplying data to another police unit for a purpose equivalent to data collection and recording

(1) A police unit may supply data from a police personal data file established for more restricted use than nationwide use to another police unit for the performance of duties laid down in section 1(1) of the Police Act if the data is necessary for the performance of the duties in question.

(2) Information as referred to in section 12 may, however, only be supplied if the information is necessary:

1) for ensuring State security;

2) for countering an immediate danger threatening life or health or for preventing significant damage to property;

3) for preventing or investigating an offence subject to imprisonment;

4) for preventing and investigating crime within the jurisdiction of the European Police Office, or some other serious crime.

(3) A police unit may supply data from a personal data file established for more restricted use than nationwide use to another police unit for the performance of duties laid down in section 1(3) of the Police Act if the data is necessary for the performance of the duty for which the data was collected and recorded.

(4) Notwithstanding any secrecy provisions, the data may also be supplied with the aid of a technical interface or in machine-readable form.

Section 18

Supplying data to another police unit for a purpose other than one equivalent to data collection and recording

(1) A police unit may supply data from a police personal data file established for more restricted use than nationwide use to another police unit for a purpose other than one equivalent to data collection and recording if the data is necessary:

1) for ensuring State security;

2) for countering an immediate danger threatening life or health or for preventing significant damage to property;

3) for preventing or investigating an offence subject to imprisonment;

4) for establishing a person's identity when undertaking an individual police duty that necessarily requires verification of identity;

5) when deciding or issuing an opinion on the granting or validity of an authorization if it has been laid down that a requirement for the granting or validity of the authorization is the applicant's or holder's reliability, suitability or other such attribute whose assessment requires information on the state of health, intoxicant use, criminal guilt or violent behaviour of the applicant or holder.

(2) Data from the Operational Data System of the Security Police referred to in section 5 and information as referred to in section 12 from a temporary personal data file as referred to in section 6(2)(2) may not, however, be supplied for the performance of the duties referred to in subsection 1(5).

(3) Data from a police personal data file may also be supplied for use in police research and planning work. Such data may also be supplied for use in police training activities if the data is essential for carrying out the training.

(4) Notwithstanding any secrecy provisions, the data may also be supplied with the aid of a technical interface or in machine-readable form.

Section 19
Supplying data to other authorities

(1) Notwithstanding any secrecy provisions, the police may supply data from police personal data files other than the Europol Data System referred to in section 30 and the National Schengen Information System referred to in section 31 with the aid of a technical interface or in machine-readable form, if the data is needed:

1) by the Finnish Vehicle Administration for the maintenance of the vehicle register in its data system of road traffic, and for the production of driving licences;

2) by the Defence Staff of the Finnish Defence Forces for the security and monitoring duties and criminal investigation referred to in the Act on the Performance of Police Tasks in the Defence Forces (1251/1995), and for conducting the background checks referred to in the Act on Background Checks (177/2002);

3) by the Frontier Guard for border surveillance, and for conducting border checks and monitoring persons' entry into and departure from the country;

4) by the Customs for monitoring international traffic, preventing and investigating customs offences, and monitoring persons' entry into and departure from the country;

5) by courts of law for handling cases concerning firearms, firearm components, cartridges or specially dangerous projectiles;

6) by courts of law for monitoring apprehension warrants, by the Probation Service and the Prison Service for monitoring apprehension warrants concerning persons sentenced to deprivation of liberty, and restraining orders, and for processing authorization matters and

monitoring compliance with authorization requirements, and by the Ministry of Justice and the military authorities for monitoring their own apprehension warrants;

7) by the Ministry for Foreign Affairs and Finland's diplomatic missions for processing matters concerning passports, visas and residence and work permits;

8) by the Directorate of Immigration for processing matters concerning Finnish citizenship, the entry into and residence in the country and employment of aliens, and refugees and asylum;

9) by public prosecutors to the extent laid down in section 11 of the Act on Public Prosecutors (199/1997);

10) by civil servants with the special police powers laid down in section 8 of the Police Act for the purpose of performing duties laid down in section 1 of the Police Act; the provisions laid down in sections 17(1-3) and 18(1-2) apply to supplying the data;

11) by the civil servants referred to in sections 1 and 6 of the Process Servers Act (505/1986) for the purpose of serving court summonses concerning passing a conversion sentence.

(2) Notwithstanding any secrecy provisions, the Supreme Police Command may, for a special reason, provide a technical interface for the Suspect Data System referred to in section 4 to civil servants of the Finnish Defence Forces, the Frontier Guard and the Customs who have been appointed to criminal intelligence or surveillance duties, and to civil servants of the Prison Service who have been appointed to criminal intelligence or surveillance duties and have the special police powers laid down in section 8 of the Police Act.

(3) Before data is supplied with the aid of a technical interface, the party requesting the data shall present an account of data security in the manner referred to in section 32(1) of the Personal Data Act.

Decisions on supplying data

(1) The decision to supply data from a police personal data file is made by the file keeper or another police unit appointed to this task by the file keeper. The police unit shall name a sufficient number of persons authorized to take decisions on supplying data from personal data files.

(2) When taking decisions on supplying data, the nature of the data to be supplied shall be taken into account in order to ensure data protection and data security for the data subject.

Section 21

Background checks

(1) When conducting a basic background check or an extended background check as referred to in the Act on Background Checks, the Security Police have the right to utilize data contained in the Data System for Police Matters, the Data System for Administrative Matters and the Operational Data System of the Security Police, and the right to obtain data contained in the judicial administration's information systems on criminal matters that are or have been subject to consideration of charges, and data contained in the criminal justice decisions register. Separate provisions shall be issued regarding the right of the Security Police to obtain other information that they could utilize when conducting a basic background check or an extended background check.

(2) When conducting a limited background check, the police have the right to utilize data contained in the Data System for Police Matters, and the right to obtain data contained in the judicial administration's information systems on criminal matters that are or have been subject to consideration of charges and data contained in the criminal justice decisions register, as well as other information that the police have the right to obtain from other authorities for this purpose, as provided elsewhere in the law.

Chapter 5

Deleting and archiving data

Section 22

Deleting data from the Data System for Police Matters

(1) Data in the Data System for Police Matters is deleted as follows:

1) in the case of apprehension warrant data, data concerning a prohibition on engaging in business is deleted five years after the end of the prohibition, data concerning a restraining order two years after the end of the order's validity, and other warrant data three years after the cancellation of the warrant;

2) searched motor vehicle data is deleted one year after the cancellation of the apprehension warrant, but in any event no later than ten years after the recording of the apprehension warrant;

3) property data is deleted one year after return of the property to its owner or holder or after its auction or destruction, but in any event no later than ten years after the recording of the data;

4) arrested persons data is deleted ten years after the recording of the most recent information; however, data on persons apprehended under section 11 of the Police Act is deleted five years after its recording;

5) crime report index and sanctions data is deleted one year after the expiry of the statute of limitations for the suspected offence; however, in the case of crime report data which has punishment or other sanction information appended to it, deletion is as follows in relation to the date on which the decision was final:

a) five years after the person was sentenced to a fine, corporate fine, juvenile punishment or dismissal;

b) ten years after the person was sentenced to a maximum of two years' imprisonment or community service;

c) twenty years after the person was sentenced to imprisonment of more than two years but no more than five years, or after the waiving of punishment under Chapter 3, section 3 of the Penal Code (39/1889);

6) message transmission data is deleted two years after the transmission of the message;

7) modus operandi data and personal descriptions data are deleted one year after:

a) the conclusion of the pre-trial investigation if it has become evident in the pre-trial investigation that no offence has been committed;

b) a decision made by the pre-trial investigation authority under section 2(2) of the Pre-trial Investigation Act to waive the measures required for the bringing of charges against the person guilty of the offence;

c) the expiry of the statute of limitations for the suspected offence if it has become evident in the pre-trial investigation that no one can be charged for the offence;

d) the file keeper was informed of the prosecutor’s decision made under Chapter 1, section 7 or 8 of the Criminal Procedure Act (689/1997) or other corresponding provision in the law to waive the measures required for the bringing of charges against the person guilty of the offence, or after the prosecutor’s decision stating that no offence has been committed or that there is no proof of an offence;

e) the file keeper was informed of a final court decision on waiving the charges brought against the data subject, or on waiving the charges on account of the expiry of the statute of limitations;

8) identification data is deleted one year after the person was found or the unidentified deceased person identified;

9) in the case of investigation and executive assistance data, crime report data is deleted one year after the expiry of the statute of limitations for the suspected offence, and other report data five years after the recording of the report; if there are several offences in the same report of an offence, the data is deleted one year after the expiry of the statute of limitations for the most recent suspected offence; if it was only possible to determine the time at which the offence was committed as a time interval, the deadline for deletion of the data is calculated from the later of the interval times.

(2) A DNA profile recorded in a police personal data file under Chapter 6, section 5 of the Coercive Measures Act is deleted from the file one year after the file keeper was informed of the prosecutor's decision stating that no offence has been committed or that there is no proof of an offence, or of waiving the charges brought against the data subject by a final court decision or of exempting the person from penal liability. If the profile is not deleted at an earlier stage, it shall be deleted no later than ten years after the data subject's death. Stored samples are destroyed at the same time as their corresponding DNA profiles are deleted.

(3) Notwithstanding the provisions of subsections 1 and 2, entries concerning persons suspected of an offence who are under 15 years of age are deleted from the data system one year after the data subject reaches 18 years of age, unless a shorter time has been laid down for deletion of the data. However, the data is not deleted on these grounds if:

1) the report concerns other suspects whose data is not yet deleted;

2) one of the entries concerns a criminal act punishable by imprisonment only; or

3) in the case of a data subject registered as a suspect of an offence when under 15 years of age, new entries are made for the person as a suspect before he or she reaches 18 years of age.

(4) Notwithstanding the provisions laid down in subsections 1 and 3, all information held on a person is deleted from the system no later than one year after the data subject's death.

(5) Notwithstanding the provisions laid down in subsections 1-4 concerning investigation and executive assistance data, identification data, property data and searched motor vehicle data, this data is not deleted if its retention is necessary for investigational or supervisory reasons related to the report in question. Personal data is not deleted either if attached to it is information concerning the person's own safety or the occupational safety of the police. The need to retain the data is reviewed no later than three years after the previous occasion on which it was reviewed, and an entry is made accordingly.

(6) Regardless of the retention period laid down in subsections 1-5, investigation and executive assistance archive data is, nevertheless, deleted 50 years after the report was recorded.

Section 23

Deleting data from the Data System for Administrative Matters

(1) Data in the Data System for Administrative Matters is deleted as follows:

1) in the case of data on firearms permits and licences, data on decisions is deleted ten years after the decision or its expiry or the end of the validity period stated in the decision, permit or licence data is deleted ten years after the end of the validity period of the permit or licence, and data on obstacles or reprimands and other recorded data are deleted ten years after the entry of the data;

2) in the case of identity card and passport data and security sector supervision data, data on decisions is deleted ten years after the decision or its expiry or the end of the validity period stated in the decision, and data on obstacles, reprimands and examinations and other recorded data are deleted ten years after the entry of the data;

3) image data is deleted three years after the end of the validity period of the administrative authorization or decision granted by the police for the preparation of which the personal photograph and specimen signature were last used;

4) local police background check data is deleted one year after a new limited background check is conducted, but in any event no later than ten years after the check;

5) aliens identification data is deleted ten years after its recording; however, if the data subject has obtained Finnish citizenship, the data is deleted one year after the file keeper was informed of the Finnish citizenship in question.

(2) All data on a person held in the data system is, however, deleted no later than one year after the data subject's death, unless there is a special reason for retaining the data. The need to retain the data is, however, reviewed no later than five years after the previous occasion on which it was reviewed, and an entry is made accordingly.

Section 24

Deleting data from the Suspect Data System

(1) Data in the Suspect Data System is deleted ten years after the last entry was made for the suspected offence.

Section 25

Deleting data from the Operational Data System of the Security Police

(1) Data on a person held in the Operational Data System of the Security Police is deleted 25 years after the last data entry was made. Data in the data system concerning basic background checks and extended background checks is deleted within one year of conducting an equivalent new background check, but in any event no later than ten years after the check.

Section 26

Deleting data from other personal data files

(1) Data in personal data files as referred to in section 6 established for the purpose of performing duties laid down in section 1(1) of the Police Act is deleted as follows:

1) in the case of manually maintained personal data files established for nationwide use by the police, the data is deleted one year after the data subject's death;

2) in the case of personal data files established for the use of a police unit or more than one police unit, the data is deleted ten years after the entry of the act, action or event, unless there is a need to retain the data for investigational or supervisory reasons; the need to retain the data is reviewed no later than three years after the previous occasion on which it was reviewed, and an entry is made accordingly.

(2) Personal data is not deleted on the grounds referred to in subsection 1 if attached to it is information concerning the person's own safety or the occupational safety of the police. The need to retain the data is reviewed no later than three years after the previous occasion on which it was reviewed, and an entry is made accordingly.

(3) In the case of personal data files as referred to in section 6 established for the purpose of performing duties laid down in section 1(3) of the Police Act, the data is deleted one year after the data subject's death.

(4) A temporary personal data file established for police use that is no longer needed shall be destroyed unless it is transferred for archiving.

Section 27
Information found to be incorrect

(1) Information found to be incorrect shall be marked as incorrect, and it may be retained if this is necessary for safeguarding the rights of the data subject, another party involved or police personnel. Such information may only be used for the stated purpose of safeguarding rights.

(2) Information found to be incorrect may not, however, be retained in the file referred to in section 31.

(3) Information found to be incorrect that is retained under subsection 1 shall be deleted as soon as there is no longer a need to retain it for the purpose of safeguarding rights, but in any event no later than five years after the end of the deadline laid down for deletion of the information.

Section 28
Archiving information

The provisions of the Archives Act (831/1994) and the provisions and orders issued under it apply to archives management functions and documents to be archived.

Chapter 6
Special provisions on processing personal data in connection with international police cooperation

Section 29
Definitions

(1) For the purposes of this Act:

1) *Europol Convention* means the Convention drawn up based on Article K.3 of the Treaty on European Union, on the Establishment of a European Police Office (Finnish Treaty Series 79/1998);

2) *European Police Office* means the police office established by the Member States of the European Union under the Europol Convention;

3) *competent Europol authorities* means the Finnish Police, the Investigation Division of the Defence Staff of the Finnish Defence Forces, the Frontier Guard and the Customs;

4) *Europol Information System* means the information system referred to in Article 7 of the Europol Convention;

5) *Schengen Convention* means the Convention implementing the Schengen Agreement between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders (Finnish Treaty Series 23/2001);

6) *Schengen States* means the signatories to the Schengen Convention and Iceland and Norway;

7) c*ompetent Schengen authorities* means the Finnish authorities mentioned in the list of competent authorities supplied by Finland to the Executive Committee referred to in Article 101(4) of the Schengen Convention which have the right, under Article 101(1-2) of the Schengen Convention, to search data entered in the Schengen Information System with the aid of a technical interface;

8) *Schengen Information System* means the information system that consists of a national section in each of the Schengen States and a technical support function; the technical support function maintains a data file which will ensure that the data files of the national sections contain identical information.

Section 30
Europol Data System

(1) The Europol Data System is a permanent, computerized personal data file intended for nationwide use by the police.

(2) The Europol Data System may include information as referred to in sections 2-4 that needs to be processed for the purpose of preventing or investigating crimine falling within the jurisdiction of the European Police Office.

(3) The competent Europol authorities may collect and record in the Europol Data System information that needs to be supplied to the Europol Information System.

(4) The police have the right to utilize data from the Europol Data System for a purpose other than one equivalent to data collection and recording if the information is necessary:

1) for ensuring State security;

2) for countering an immediate danger threatening life or health or for preventing significant damage to property;

3) for preventing or investigating an offence subject to imprisonment.

Section 31
National Schengen Information System

(1) The National Schengen Information System is a permanent, computerized personal data file intended for nationwide use by the police.

(2) The following may constitute a sub-file of the National Schengen Information System:

1) the national section of the Schengen Information System; and

2) the Schengen Record File.

(3) Provisions on the purpose of use and information content of the national section of the Schengen Information System are laid down in Articles 92-100 of the Schengen Convention.

(4) The competent Schengen authorities may collect and record in the Schengen Record File information that needs to be supplied to the Schengen Information System for purposes laid down in Articles 95-100 of the Schengen Convention.

(5) The police have the right to utilize data from the National Schengen Information System for a purpose other than one equivalent to data collection and recording, as laid down in Article 102 of the Schengen Convention.

Section 32

Data file maintained by the technical support function of the Schengen Information System

(1) Provisions on the data file maintained by the technical support function of the Schengen Information System are laid down in Titles IV and VI of the Schengen Convention.

Section 33

Right to obtain data from the Europol Information System

(1) Provisions on the right of the Finnish Police, the Investigation Division of the Defence Staff of the Finnish Defence Forces, the Frontier Guard and the Customs to obtain data from the Europol Information System are laid down in Articles 2 and 17 of the Europol Convention.

(2) Data from the Europol Information System shall be obtained through the National Bureau of Investigation.

Section 34

Right of the police to obtain data from the Schengen Information System

(1) Provisions on the right of the police to obtain data from the Schengen Information System are laid down in Articles 101 and 102 of the Schengen Convention.

Section 35

Supplying data from the Europol Data System

(1) The police may supply data from the Europol Data System referred to in section 30 to the competent Europol authorities for purposes laid down in Articles 4-9 of the Europol Convention.

(2) The police may supply data from the Europol Data System to the competent Europol authorities for a purpose other than one equivalent to data collection and recording if the data is necessary:

1) for ensuring State security;

2) for countering an immediate danger threatening life or health or for preventing significant damage to property;

3) for preventing or investigating an offence subject to imprisonment.

(3) Notwithstanding any secrecy provisions, the police may also supply the data with the aid of a technical interface or in machine-readable form.

Section 36

Supplying data from the National Schengen Information System

(1) The police may supply data from the National Schengen Information System referred to in section 31 to the competent Schengen authorities for purposes laid down in Articles 95-100 of the Schengen Convention. The police may supply data recorded in the information system to the competent Schengen authorities for a purpose other than one equivalent to data collection and recording as laid down in Article 102 of the Schengen Convention.

(2) Notwithstanding any secrecy provisions, the police may also supply the data with the aid of a technical interface or in machine-readable form.

Section 37

Supplying data within the Member States of the European Union and within the European Economic Area

(1) The police may supply data from a police personal data file established for the purpose of performing duties laid down in section 1(1) of the Police Act to police authorities and other authorities within the Member States of the European Union and within the European Economic Area whose duties include securing judicial and social order, maintaining public order and security or preventing or investigating offences and

forwarding them to a prosecutor for consideration of charges, if the data is essential for performing the duties in question. Data from a police personal data file established for the purpose of performing duties laid down in section 1(3) of the Police Act may be supplied if the data is essential for the performance of the duty for which the data was collected and recorded.

(2) Information as referred to in section 12 may, however, only be supplied if it is essential:

1) for ensuring State security;

2) for countering an immediate danger threatening life or health or for preventing significant damage to property;

3) for preventing or investigating an offence subject to imprisonment.

4) for preventing and investigating crime falling within the jurisdiction of the European Police Office, or some other serious crime.

(3) The police may supply data from a police personal data file to the authorities referred to in subsection 1 for a purpose other than one equivalent to data collection and recording if the data is essential:

1) for ensuring State security;

2) for countering an immediate danger threatening life or health or for for preventing significant damage to property;

3) for preventing or investigating an offence subject to imprisonment.

4) for establishing a person’s identity when undertaking an individual police duty that necessarily requires verification of identity;

5) for deciding or issuing an opinion on the granting or validity of an authorization if it has been laid down that a requirement for the granting or validity of the authorization is the applicant’s or holder’s reliability, suitability or other such attribute whose assessment

requires information on the state of health, intoxicant use, criminal guilt or violent behaviour of the applicant or holder.

(4) Data from the Operational Data System of the Security Police referred to in section 5 and data as referred to in section 12 from a file as referred to in section 6(2)(2) that is temporary may not, however, be supplied for the performance of the duties referred to in subsection 3(5).

(5) Data from the Suspect Data System referred to in section 4 may not, however, be supplied for the performance of the duties referred to in subsection 3(5).

(6) Notwithstanding any secrecy provisions, the data may also be supplied with the aid of a technical interface or in machine-readable form.

(7) Before supplying data with the aid of a technical interface, the party requesting the data shall present an account of data security in the manner referred to in section 32(1) of the Personal Data Act.

Section 38

Supplying data to the European Police Office

(1) The police may supply data from a police personal data file to the European Police Office and the national units of the European Police Office, and for recording in the Europol Information System, for the prevention and investigation of crime falling within the jurisdiction of the European Police Office. The data shall be supplied through the National Bureau of Investigation.

(2) Notwithstanding any secrecy provisions, the National Bureau of Investigation may also supply the data to the Europol Information System with the aid of a technical interface or in machine-readable form.

Section 39

Supplying data to a Schengen State and to the Schengen Information System

(1) The police may supply from a police personal data file data as referred to in Article 94 of the Schengen Convention that is necessary for the purposes laid down in Articles 95-100 of the Schengen Convention to the competent authorities of Schengen States and for recording in the Schengen Information System. The data shall be supplied through the National Bureau of Investigation.

(2) Notwithstanding any secrecy provisions, the National Bureau of Investigation may also supply the data with the aid of a technical interface or in machine-readable form.

Section 40

Other supplying of data abroad

(1) The police may supply data from a police personal data file, subject to the conditions laid down in section 37(1-4), to the International Criminal Police Organization (ICPO–Interpol) or to the police authorities of the Member States of Interpol other than those referred to in section 37, or to other authorities in such States whose duties include securing judicial and social order, maintaining public order and security, or preventing or investigating offences and forwarding them to a prosecutor for consideration of charges.

(2) The police may supply data from a police personal data file to the police authorities of States other than those referred to in subsection 1, or to other authorities in such States whose duties include securing judicial and social order, maintaining public order and security, or preventing or investigating offences and forwarding them to a prosecutor for consideration of charges. The data may be supplied if it is essential:

1) for ensuring State security;

2) for countering an immediate danger threatening life or health or for preventing significant damage to property;

3) for preventing or investigating an offence subject to imprisonment.

(3) The police may supply data from a police personal data file concerning the acquisition, possession, transfer, import and export of firearms, firearm components, cartridges or specially dangerous projectiles to an arms control authority of another State if the supplying of the data is essential for arms control.

Section 41
Deleting data from the Europol Data System

(1) The provisions of Article 21 of the Europol Convention shall be observed when deleting data from the Europol Data System.

(2) If personal data that has been supplied to the Europol Information System is deleted from the data system, the European Police Office shall be notified of the deletion of the data.

Section 42
Deleting data from the National Schengen Information System

(1) The provisions of Articles 112 and 113 of the Schengen Convention shall be observed when deleting data from the National Schengen Information System.

Chapter 7
Rights of data subjects

Section 43
Providing information about the processing of data

When collecting personal data for the purpose of performing duties as referred to in section 1(3) of the Police Act, the police shall be mindful of their obligation to provide information under section 24(1) of the Personal Data Act. This obligation does not apply when the police are collecting, recording or supplying personal data necessary for the performance of duties as referred to in section 1(1) of the Police Act.

Section 44
Right of access

(1) The provisions of sections 26 and 28 of the Personal Data Act apply to the application of the right of access. The data to be accessed is provided by the file keeper. Data to be accessed from a personal data file established for nationwide use by the police may also be provided by some other police unit specified by the file keeper. The police unit shall name a sufficient number of persons authorized to take decisions in regard to the application of the right of access and the related provision of data.

(2) When applying their right of access, data subjects shall present a request to this effect in person to the file keeper or some other police unit as referred to in subsection 1 and prove their identity.

Section 45
Restricting the right of access

(1) The right of access does not apply in any way to:

1) data in the Suspect Data System;

2) data in the Europol Data System;

3) data in the Operational Data System of the Security Police;

4) data in the National Schengen Information System in cases as referred to in Article 109(2) of the Schengen Convention;

5) classification, surveillance or modus operandi data concerning persons or acts included in other police personal data files.

(2) At the request of the data subject, the Data Protection Ombudsman may examine the lawfulness of the data referred to in subsection 1 that is held on the data subject.

(3) The provisions of section 27 of the Personal Data Act also apply to restrictions on the right of access.

Section 46

Applying the right of access to data in the Europol Information System

(1) The European Police Office provides the data to be accessed from the Europol Information System. A request to this effect shall be presented to the District Police, which forward the matter without delay for processing by the European Police Office. The District Police shall notify the person submitting the request that the European Police Office will reply to him or her directly.

(2) Everyone has the right to ask the Data Protection Ombudsman to verify the lawfulness of any information on themselves that the National Bureau of Investigation has recorded in the Europol Information System and transmitted to the European Police Office, and the utilization of that information.

(3) Everyone also has the right to ask the Europol Joint Supervisory Body to verify that the collection, recording, processing and utilization by the European Police Office of personal data on themselves occur in a lawful and correct manner. A request to this effect shall be presented to the Data Protection Ombudsman or the District Police, which shall forward the matter without delay for processing by the Europol Joint Supervisory Body.

(4) The request referred to in subsection 1 concerning access to data and the request to be presented to the District Police referred to in subsection 3 concerning verification of data shall be presented to the District Police in person, and at the same time the person presenting the request shall prove his or her identity.

(5) The Data Protection Ombudsman has the right to have access to the Europol Information System for monitoring that the recording and utilization of personal data necessary for preventing and investigating crime falling within the jurisdiction of the European Police Office in the information system and its transmission to the European Police Office occur in a lawful manner and without violating the rights of the individual.

Section 47

Applying the right of access to data in the data file maintained by the technical support function of the Schengen Information System

(1) Everyone has the right to ask the supervisory authority referred to in Article 115 of the Schengen Convention to verify that the collection, recording, processing and utilization of personal data on themselves in the data file maintained by the technical support function of the Schengen Information System occur in a lawful and correct manner. A request to this effect shall be presented to the Data Protection Ombudsman or the District Police. The police shall forward any verification request presented to the District Police to the Data Protection Ombudsman without delay.

(2) The verification request presented to the District Police referred to in subsection 1 shall be presented in person, and at the same time the person presenting the request shall prove his or her identity.

Chapter 8
Miscellaneous provisions

Section 48

Further provisions and instructions

(1) Further provisions on the procedures for providing a technical interface as referred to in section 19 of this Act, for deciding on supplying data as referred to in section 20, and for applying the right of access referred to in section 44 may be given by government decree.

(2) The Supreme Police Command may issue further instructions under this Act or provisions issued under it on the undertaking of actions by the police. The Supreme Police Command confirms the format of the administrative forms to be used for these actions.

Section 49

Entry into force

(1) This Act comes into force on 1 October 2003.

(2) This Act repeals the Police Personal Data File Act (509/1995) of 7 April 1995, as amended.

(3) Measures necessary for the implementation of this Act may be undertaken before the Act's entry into force.

Entry into force and application of amendments:

(523/2004) This Act comes into force on 1 September 2004.