Privacy statement; National Schengen Information System

1 Controller

National Police Board
Postal address: P.O. Box 1000, 02151 Espoo
Street address: Vuorimiehentie 3, Espoo
Telephone: +358 (0)295 480 181 (exchange)
Email: kirjaamo.poliisihallitus@poliisi.fi

2 Contact person in data protection matters

National Police Board
Päivi Laaksonen, Senior Adviser
Contact address: See section 1

3 Data Protection Officer of the Police

National Police Board
Harri Kukkola, Senior Adviser
Contact address: See section 1

4 Legal grounds for processing personal data

The Police process personal data to discharge their statutory duties, to fulfil their legal obligations and to exercise the public authority vested in the Police when the preconditions set out in data protection legislation are met. According to data protection legislation, legal obligations can only be based on the law of the European Union or a Member State, and the public authority must have been attributed in statutory laws or other legal regulations.

Provision on the processing of personal data by the Police and the legal grounds for the processing relating to the National Schengen Information System are set out in the following laws: Act on the Processing of Personal Data by the Police

(616/2019, hereinafter the Police Personal Data Act), Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security (1054/2018, hereinafter the Act on Data Protection in Criminal Matters), and in the SIS regulations.

The SIS regulations refer to the following Regulations of the European Parliament and of the Council:

- Regulation (EU) 2018/1860 of the European Parliament and of the Council on the use of the Schengen Information System for the return of illegally staying third-country nationals (hereinafter “Regulation on returns”)
- Regulation (EU) 2018/1861 of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006 (hereinafter “Regulation on border checks”)
- Regulation (EU) 2018/1862 of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of Police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU (hereinafter “Regulation on Police cooperation”)

5 Purpose of the processing of personal data, the categories of data subjects and the categories of personal data being processed

The purpose of the Schengen Information System (SIS) is to ensure a high level of security within the area of freedom, security and justice of the Union, by promoting the operative cooperation between the national competent authorities. The Schengen Information System is an information exchange system where the competent authorities of the Schengen countries store and search information on wanted or missing persons, missing or stolen property as well as on notices of return decisions and refusals of entry or stay in the country.

The data entered in the Schengen system includes warrants related to persons and objects and related personal data in eight alert categories in line with the Regulations on returns, border checks and Police cooperation.

The alert categories are the following:

- Alerts on returns in accordance with the Regulation on returns, to be entered in the SIS system on third-country nationals who are subject to a return decision in order to ensure that the return obligation has been followed and to support the implementation of the return decisions.
- Alerts on third-country nationals entered in accordance with the Regulation on border checks stored in view of refusing entry and stay in a country.
- In line with the Regulation on Police cooperation, the alert types and uses are the following:
  - Based on Article 26, alerts on person wanted for arrest for surrender on the basis of a European Arrest Warrant or alerts on persons wanted for arrest for extradition purposes.
  - Based on Article 32, alerts on missing persons or vulnerable persons who need to be prevented from travelling.
  - Based on Article 34, alerts on persons sought to be summoned to appear before the judicial authorities.
  - Based on Article 36, alerts on persons and objects for discreet checks, or checks for investigating and special purposes.
  - Based on Article 38, alerts on objects sought for the purposes of seizure or for use as evidence in criminal proceedings.
  - Based on Article 40, alerts on wanted persons for the purposes of identification under national law.

5.1 Alerts entered on the basis of the Regulation on returns

According to the Regulation on returns, the alerts shall contain only the following data:

a) surnames
b) forenames
c) names at birth
d) previously used names and aliases
e) place of birth
f) date of birth
g) gender
h) any nationalities held
i) whether the person concerned
   - is armed
   - is violent
   - as absconded or escaped

- poses a risk of suicide
- poses a threat to public health
- is involved in terrorist operations

j) the reason for the alert
k) the authority which created the alert
l) a reference to the decision giving rise to the alert
m) the action to be taken in the case of a hit
n) links to other alerts
o) whether the return decision is issued in relation to a third-country national who popes a threat to public policy, to public security or to national security
p) the type of offence
q) the category of the person's identification documents
r) the country of issue of the person's identification documents
s) the number(s) of the person's identification documents
t) the date of issue of the person's identification documents
u) photographs and facial images
v) dactyloscopic (fingerprint) data
w) copy of the identification documents, in colour wherever possible
x) last date of the period for voluntary departure, if granted
y) whether the return decision has been suspended of the enforcement of the decision has been postponed, including as a result of the lodging of an appeal
z) whether the return decision is accompanied by an entry ban constituting the basis for an alert for refusal or entry and stay.

5.2 Alerts entered on the basis of the Regulation on border checks

Alerts on third-country nationals made in accordance with the Regulation on border checks entered in view of refusing entry and stay in a country shall contain only the following data:

a) surnames
b) first names
c) names at birth
d) previously used names and aliases
e) any specific, objective, physical characteristics not subject to change
f) place of birth
g) date of birth

h) gender
i) any nationalities held
j) whether the person concerned
   - is armed
   - is violent
   - as absconded or escaped
   - poses a risk of suicide
   - poses a threat to public health
   - is involved in terrorist operations
k) reason for alert
l) the authority which created the alert
m) reference to decision giving rise to alert
n) the action to be taken in the case of a hit
o) links to other alerts
p) whether the person concerned is a family member of a citizen of the Union or other person who is a beneficiary of the right of free movement as referred to in Article 26
q) whether the decision for refusal of entry and stay is based on
   - previous conviction
   - a serious security threat
   - circumvention of Union or national law on entry and stay
   - an entry ban or
   - a restrictive measure
r) the type of offence
s) the category of the person's identification document(s)
t) the country of issue of the person's identification documents
u) the number(s) of the person's identification document(s)
v) the date of issue of the person's identification document(s)
w) photographs and facial images
x) dactyloscopic data
y) copy of the identification documents, in colour wherever possible

5.3 Alerts entered on the basis of the Regulation on Police cooperation

Only the following personal data of the person covered by an alert shall be entered in SIS:

a) surnames
b) first names

c) names at birth
d) previously used names and aliases
e) any specific, objective, physical characteristics not subject to change
f) place of birth
g) date of birth
h) gender
i) any nationalities held
j) whether the person concerned
   - is armed
   - is violent
   - has absconded or escaped
   - poses a risk of suicide
   - poses a threat to public health
   - is involved in terrorist operations
k) reason for alert
l) the authority which created the alert
m) reference to decision giving rise to alert
n) the action to be taken in the case of a hit
o) links to other alerts
p) the type of offence
q) the person's registration number in the national register
r) information on the type of case concerned when the alert is on missing persons or vulnerable persons who need to be prevented from travelling
s) the category of the person's identification documents
t) the country of issue of the person's identification documents
u) the number(s) of the person's identification document(s)
v) the date of issue of the person's identification document(s)
w) photographs and facial images
x) DNA profiles
y) dactyloscopic data
z) copy of the identification documents, in colour wherever possible

5.3.1 Alerts on person wanted for arrest for surrender on the basis of a European Arrest Warrant or alerts on persons wanted for arrest for extradition purposes.

The alerts under Article 26 are entered at the request of the judicial authority of the issuing Member State. Where a person is wanted for arrest for surrender purposes on the basis of a European Arrest Warrant, the issuing Member State shall enter into SIS a copy of the original of the European Arrest Warrant.

5.3.2 Alerts on missing persons or vulnerable persons who need to be prevented from travelling.

Based on Article 32, alerts on missing persons or vulnerable persons who need to be prevented from travelling shall be entered on persons of the following categories:

a) missing persons who need to be placed under protection
b) missing persons who do not need to be placed under protection
c) children at risk of abduction by a parent, a family member or a guardian, who need to be prevented from travelling
d) children who need to be prevented from travelling owing to a concrete and apparent risk of them being removed from or leaving the territory of a Member State and becoming victims of trafficking in human beings, or of forced marriage, female genital mutilation or other forms of gender-based violence or becoming victims of or involved in terrorist offences of becoming conscripted or enlisted into armed groups or being made to participate actively in hostilities
e) vulnerable persons who are of age and who need to be prevented from travelling for their own protection owing to a concrete and apparent risk of them being removed from or leaving the territory of a Member State and becoming victims of trafficking in human beings or gender-based violence

A DNA profile shall be added to on missing persons who need protection only following a quality check to ascertain whether the minimum data quality standards and technical specifications have been met and only where photographs, facial images or dactyloscopic data are not available or not suitable for identification. The DNA profiles of persons who are direct ascendants, descendants or siblings of the subject of the alert shall be added to the alert provided that those persons give their explicit consent. Where a DNA profile is added to an alert, that profile shall contain the minimum information strictly necessary for the identification of the missing person.

5.3.3 Alerts on persons sought to be summoned to appear before the judicial authorities

Based on Article 34, alerts on persons sought to be summoned to appear before the judicial authorities shall contain data on:

a) witnesses

b) persons summoned or persons sought to be summoned to appear before the judicial authorities in connection with criminal proceedings in order to account for acts for which they are being prosecuted
c) persons who are to be served with a criminal judgment or other documents in connection with criminal proceedings in order to account for acts for which they are being prosecuted
d) persons who are to be served with a summons to report in order to serve a penalty involving a deprivation of liberty.

5.3.4 Alerts on persons and objects for discreet checks, inquiry checks or specific checks

Alerts under Article 36 on persons for discreet checks, inquiry checks or specific checks shall be entered for the purposes of preventing, detecting, investigating or prosecuting criminal offences, executing a criminal sentence and preventing threats to public security. For the above purposes, the executing Member State shall collect and communicate to the issuing Member State all or some of the following information:

a) the fact that the person who is object of an alert, or that objects referred to in an alert, has been located
b) the place, time and reason for the check
c) the route of the journey and destination
d) the persons accompanying the subject of the alert or the occupants of the vehicle, boat or aircraft, or the persons accompanying the holder of the blank official document or issued identity document who can reasonably be expected to be associated with the subject of the alert
e) any identity revealed and any personal description of the person using the blank official document or issued identity document that is the subject of the alert
f) the objects referred to in points (a), (b), (c), (e), (g), (h), (j), (k) and (l) in the next chapter of this policy or non-cash means of payment used
g) any objects carried, including travel documents
h) the circumstances in which the person or the objects referred to in points (a), (b), (c), (e), (g), (h), (j), (k) and (l) in the next chapter of this policy or the non-cash means of payment were located
i) any other information being sought by the issuing Member State in accordance with Article 36.

5.3.5 Alerts on objects sought for the purposes of seizure or for use as evidence in criminal proceedings

Under Article 38 of the Regulation on Police cooperation, the alerts for the purposes of seizure or for use as evidence in criminal proceedings are entered on the following categories of readily identifiable objects:

a) motor vehicles regardless of the propulsion system
b) trailers with an unladen weight exceeding 750 kg
c) caravans
d) industrial equipment
e) boats
f) boat engines
g) containers
h) aircraft
i) aircraft engines
j) firearms
k) blank official documents which have been stolen, misappropriated, lost or purport to be such a document but are false
l) issued identity documents, such as passports, identity cards, residence permits, travel documents and driving licences which have been stolen, misappropriated, lost or invalidated or purport to be such a document but are false
m) vehicle registration certificates and vehicle number plates which have been stolen, misappropriated, lost or invalidated or purport to be such a document or plate but are false
n) banknotes (registered notes) and false banknotes
o) items of information technology
p) identifiable component parts of motor vehicles
q) identifiable component parts of industrial equipment
r) other identifiable objects of high value.

5.3.6 Alerts on unknown wanted persons for the purposes of identification under national law

Under Article 40 of the Regulation on Police cooperation, alerts on unknown wanted persons can be entered in the SIS system, containing dactyloscopic data. Such dactyloscopic data shall be either complete or incomplete sets of fingerprints or palm prints discovered at the scenes of terrorist offences or other serious crimes under investigation. They shall only be entered into SIS where it can be established to a very high degree of probability that they belong to a

perpetrator of the offence. Moreover, the alert can only be entered if the competent authority cannot establish the identity of the suspect on the basis of data from any other relevant national, Union or international database.

5.3.7 Additional data for the purpose of dealing with misused identity

Where confusion shall arise between the person intended to be the subject of an alert and a person whose identity has been misused, the issuing Member State shall, subject to the explicit consent of the person whose identity has been misused, add data relating to the latter to the alert in order to avoid the negative consequences of misidentification. Any person whose identity has been misused shall have the right to withdraw his or her consent regarding the processing of the added personal data.

Data relating to a person whose identity has been misused may only be used for the following purposes: a) to allow the competent authority to distinguish the person whose identity has been misused from the person intended to be the subject of the alert; andb) to allow the person whose identity has been misused to prove his or her identity and to establish that his or her identity has been misused.

For the purpose of this Article, and subject to the explicit consent of the person whose identity has been misused for each data category, only the following personal data of the person whose identity has been misused may be entered and further processed in SIS:

a) surnames
b) forenames
c) names at birth
d) previously used names and any aliases possibly entered separately
e) any specific, objective, physical characteristics not subject to change
f) place of birth
g) date of birth
h) gender
i) photographs and facial images
j) fingerprints, palm prints or both
k) any nationalities held
l) the category of the person’s identification document(s)
m) the country of issue of the person’s identification document(s)
n) the number(s) of the person’s identification document(s)

o) the date of issue of the person's identification document(s)
p) address of the person
q) person's father's name
r) person's mother's name

5.3.8 Supplementary information

The SIRENE Bureaus in the Schengen area exchange information on the alerts. Such exchange of information is referred to as exchange of supplementary information. Supplementary information shall include, for example, details of the surrender arrangements of the persons under alert, or information of a person under alert being found.

The supplementary information form under the alert referred to in Article 26 and the European Arrest Warrant entered in the alert can make reference to the person's race or ethnic origin, political opinion, religion or philosophical belief, trade union membership, sexual orientation or behaviour if this has been the reason for the crime against the individual and it has been described, for that reason, in the description of the crime or as a part of the circumstances in which the crimes have been committed.

6 Regular disclosure of information

Notwithstanding the non-disclosure provisions, the Police shall disclose the information in the National Schengen Information System to the Finnish Security Intelligence Service, the Boarder Guard, the Customs, the Defence Forces, the prosecutors, the Finnish Immigration Service, the Finnish Transport and Communications Agency, the Emergency Response Centre Agency, the Ministry for Foreign Affairs as well as Finnish diplomatic mission, with due respect of the provisions in the SIS Regulations. The data may also be disclosed by means of a technical connection, or as a set of data.

The supplementary information referred to in the Schengen Information System Regulations shall be disclosed via the SIRENE Bureau. The National Bureau of Investigations serves as the SIRENE Bureau in Finland.

The Member States shall notify the European Union Agency for Law Enforcement Cooperation (Europol) of any hits for alerts related to terrorist crimes. As an exception, the Member States may omit to inform Europol of a hit, if the notification would endanger an ongoing investigation or a person's security

or would be against the pertinent security interests of the Member State that has made the alert.

7 Erasing and archiving of personal data

7.1 Period of validity of alerts

As a premise, the period of validity entered for an alert is its maximum duration. In alerts under Article 26 on person wanted for arrest for surrender on the basis of a European Arrest Warrant or alerts on persons wanted for arrest for extradition purposes, the period of validity is determined on the basis of the prosecution limitation date. The alert is erased when the prosecution falls under the statute of limitations.

The SIRENE Bureau follows the alerts close to becoming time-barred and extends the period of validity of the alerts made, reminding and asking the alerting authority whether an extension of the alert is needed. If necessary, each Member State can issue legislation on shorter periods of review based on their national legislation. The Member State issuing the alert shall, during the review period related to the alert, decide on the basis of an individual assessment recorded in a log record, to retain an alert on a person in force longer than the review period if the retention is necessary and proportionate in view of the objectives for which the alert was entered.

Alerts on persons will be automatically erased at the end of the review period, unless the alerting Member State has communicated that the validity is extended.

7.1.1 Validity periods determined for alerts on persons

Alerts on persons may be kept only for the time required to achieve the purpose for which they were entered.

The alerts that can be entered for the period of five years include:

- alerts related to returns
- alerts on third-country nationals entered in view of refusing entry and stay in a country
- alerts on missing persons with the need to be place under protection
- alerts on missing persons with no need to be place under protection

The alerts that can be entered for the period of three years include:

- Alerts on persons sought to be summoned to appear before the judicial authorities
- Alerts on wanted persons for the purposes of identification under national law.

The alerts that can be entered for the period of one year include:

- alerts on children at risk of abduction by a parent, a family member or a guardian, who need to be prevented from travelling
- alerts on children who need to be prevented from travelling owing to a concrete and apparent risk of them being removed from or leaving the territory of a Member State and becoming victims of trafficking in human beings, or of forced marriage, female genital mutilation or other forms of gender-based violence or becoming victims of or involved in terrorist offences of becoming conscripted or enlisted into armed groups or being made to participate actively in hostilities
- alerts on vulnerable persons who are of age and who need to be prevented from travelling for their own protection owing to a concrete and apparent risk of them being removed from or leaving the territory of a Member State and becoming victims of trafficking in human beings or gender-based violence
- alerts on persons and objects for discreet checks, or checks for investigating and special purposes

7.1.2 Validity periods determined for alerts on objects

The Member State can enter a one-year alert on the following objects for discreet checks, inquiry checks and specific checks:

- blank official documents which have been stolen, misappropriated, lost or purport to be such a document but are false
- issued personal documents, such as passports, personal ID cards, residence permits, travel documents as well as drivers' licences, stolen or misappropriated, invalidated or purport to be such documents but false
- motor vehicles regardless of the propulsion system
- trailers with an unladen weight exceeding 750 kg
- caravans
- boats
- containers
- aircraft
- firearms

The alerts under Article 38 of the Regulation on Police cooperation on travel documents invalidated by the authorities and the alerts on objects for seizure or for use as evidence in criminal proceedings, can be entered for ten years on the following objects, with the exception of containers, the validity of which is five years and items of information technology, with the validity of one year:

- travel documents invalidated by the authorities
- motor vehicles regardless of the propulsion system
- trailers with an unladen weight exceeding 750 kg
- caravans
- industrial equipment
- boats
- boat engines
- containers
- aircraft
- aircraft engines
- firearms
- blank official documents which have been stolen, misappropriated, lost or purport to be such a document but are false
- issued personal documents, such as passports, personal ID cards, residence permits, travel documents as well as drivers' licences, stolen or embezzled, invalidated or looking like such documents but false
- vehicle registration certificates and vehicle number plates which have been stolen, misappropriated, lost or invalidated or purport to be such a document or plate but are false
- banknotes (registered notes) and false banknotes
- items of information technology
- identifiable component parts of motor vehicles
- identifiable component parts of industrial equipment

7.2 Erasing alerts

7.2.1 Alerts on returns

Alerts on return should be deleted as soon as the Member State receives confirmation that the return has taken place. If necessary, the alert on a refusal of entry and stay shall be entered at the same time without delay. In the event of a hit on an alert on return concerning a third-country national who is entering the territory of the Member States through the external border of a Member State, and the issuing Member State is informed of such circumstances, it shall

immediately delete the alert on return and enter an alert for refusal of entry and stay.

Where the granting Member State notifies the issuing Member State that it intends to grant or extend the residence permit or long-stay visa or that it has decided to do so, the issuing Member State shall delete the alert on return.

Where a Member State considers granting or extending a residence permit or long-stay visa to a third-country national who is the subject of an alert on return entered by another Member State which is not accompanied by an entry ban, the granting Member State shall inform without delay the issuing Member State that it intends to grant or has granted a residence permit or a long-stay visa. The issuing Member State shall delete the alert on return without delay.

If it has emerged that a Member State has entered a return alert on a third-country national who has a valid residence permit or long-term visa granted by another Member State, the alerting Member State may decide to withdraw the return decision. In case of such a withdrawal, it will immediately delete the alert on return. Where the granting Member State notifies the issuing Member State that it intends uphold a residence permit or long-stay visa, the issuing Member State shall delete the alert on return.

In addition to the above, alerts on return shall be deleted when the decision on the basis of which the alert was entered has been withdrawn or annulled by the competent authority. Alerts on returns shall also be deleted when the third-country national in question can prove to have left the Member State territory in line with the return decision. Alerts on return concerning a person who has acquired citizenship of a Member State or of any State whose nationals are beneficiaries of the right of free movement under Union law shall be deleted as soon as the issuing Member State becomes aware or is so informed pursuant to Article 44 of Regulation (EU) 2018/1861 that the person in question has acquired such citizenship.

7.3 Alerts entered on the basis of the Regulation on border checks

Alerts in accordance with the Regulation on border checks stored in view of refusing entry and stay in a country shall be deleted:

- when the competent authorities have withdrawn or cancelled the decision constituting the basis for entering the alert or

- where the consultation preceding the granting or extending of the residence permit or long-stay visa results in the granting Member State notifying the issuing Member State that it intends to grant or extend the residence permit or long-stay visa, the issuing Member State shall delete the alert on entry or stay in the country.
- Where it emerges that a Member State has entered an alert for refusal of entry and stay on a third-country national who is the holder of a valid residence permit or long-stay visa granted by another Member State, and the granting Member State informs the issuing Member State, after consultation, that it will uphold the residence permit or long-stay visa, the issuing Member State shall immediately delete the alert for refusal or entry and stay.
- Alerts on third-country nationals who are the subject of a restrictive measure intended to prevent entry into or transit through the territory of Member States shall be deleted when the restrictive measure has been terminated, suspended or annulled.
- Alerts on return concerning a person who has acquired citizenship of a Member State or of any State whose nationals are beneficiaries of the right of free movement under Union law shall be deleted as soon as the issuing Member State becomes aware or is so informed pursuant to Article 44 of Regulation (EU) 44 that the person in question has acquired such citizenship.
- Alerts shall be deleted upon expiry of the alert unless the issuing Member State has communicated that it will be extended. If the issuing Member State has not given information on the extension of the alert, the alert will be automatically deleted after the period of validity.

7.4 Erasing alerts based on Regulation on Police cooperation

Alerts on objects shall be kept only for the time required to achieve the purpose for which they were entered. The Member State issuing the alert may, during the review period related to the alert, decide on the basis of an individual assessment recorded in a log record, to keep an alert on an object in force longer than the review period if it is necessary and proportionate in view of the objectives for which the alert was entered. When an alert on an object is linked to an alert on a person, it shall be reviewed pursuant to Article 53. Such alerts shall only be kept for as long as the alert on the person is kept.

Alerts for arrest for surrender or extradition purposes pursuant to Article 26 shall be deleted when the person has been surrendered or extradited to the competent authorities of the issuing Member State.

Alerts shall be deleted upon expiry of the alert unless the issuing Member State has communicated that it will be extended. If the issuing Member State has not given information on the extension of the alert, the alert will be automatically deleted after the period of validity. They shall also be deleted when the judicial decision on which the alert was based has been revoked by the competent judicial authority in accordance with national law.

Alerts concerning missing children and children at risk of abduction shall be deleted upon

- the resolution of the case, such as when the child has been located or repatriated or the competent authorities in the executing Member State have taken a decision on the care of the child
- the expiry of the alert unless the issuing Member State has communicated that it will be extended. If the issuing Member State has not given information on the extension of the alert, the alert will be automatically deleted after the period of validity or
- the competent authority in the issuing Member State has taken a decision in the case.

Alerts on missing adults where no protective measures are requested, shall be deleted upon

- the execution of the action to be taken, where their whereabouts are ascertained by the executing Member State
- the expiry of the alert unless the issuing Member State has communicated that it will be extended. If the issuing Member State has not given information on the extension of the alert, the alert will be automatically deleted after the period of validity or
- the competent authority in the issuing Member State has taken a decision in the case.

Alerts on missing adults where protective measures are requested, shall be deleted upon

- the carrying out of the action to be taken, where the person is placed under protection
- the expiry of the alert unless the issuing Member State has communicated that it will be extended. If the issuing Member State has not given information on the extension of the alert, the alert will be automatically deleted after the period of validity or

- the competent authority in the issuing Member State has taken a decision in the case.

Alerts on vulnerable persons who are of age who need to be prevented from travelling for their own protection and children who need to be prevented from travelling, an alert shall be deleted upon

- the carrying out of the action to be taken such as the person's placement under protection
- the expiry of the alert unless the issuing Member State has communicated that it will be extended. If the issuing Member State has not given information on the extension of the alert, the alert will be automatically deleted after the period of validity or
- the competent authority in the issuing Member State has taken a decision in the case.

Without prejudice to the national law, where a person has been institutionalised following a decision by a competent authority an alert may be retained until that person has been repatriated.

Alerts on persons sought for a judicial procedure pursuant to Article 34 shall be deleted upon

a) the communication of the whereabouts of the person to the competent authority of the issuing Member State
b) the expiry of the alert unless the issuing Member State has communicated that it will be extended. If the issuing Member State has not given information on the extension of the alert, the alert will be automatically deleted after the period of validity or
c) the competent authority in the issuing Member State has taken a decision in the case.

Alerts for discreet, inquiry and specific checks pursuant to Article 36, shall be deleted upon

a) the expiry of the alert unless the issuing Member State has communicated that it will be extended. If the issuing Member State has not given information on the extension of the alert, the alert will be automatically deleted after the period of validity or
b) a decision to delete them by the competent authority of the issuing Member State.

Alerts on objects for seizure or use as evidence in criminal proceedings pursuant to Article 38, shall be deleted upon

a) the seizure of the object or equivalent measure once the necessary follow-up exchange of supplementary information has taken place between the SIRENE Bureaus concerned or the object becomes the subject of another judicial or administrative procedure
b) the expiry of the alert unless the issuing Member State has communicated that it will be extended. If the issuing Member State has not given information on the extension of the alert, the alert will be automatically deleted after the period of validity or
c) a decision to delete them by the competent authority of the issuing Member State.

Alerts on unknown wanted persons pursuant to Article 40 shall be deleted upon

a) the identification of the person
b) the expiry of the alert unless the issuing Member State has communicated that it will be extended. If the issuing Member State has not given information on the extension of the alert, the alert will be automatically deleted after the period of validity or
c) a decision to delete them by the competent authority of the issuing Member State.

Erroneous information retained to safeguard the rights of a data subject, other interested party or Police personnel, will be immediately deleted as soon as the retaining of such information is no longer necessary to safeguard the rights.

Supplementary information for the purpose of dealing with misused identities shall be deleted at the same time as the corresponding alert, or earlier if the person whose identity has been misused, demands it.

Personal date held by a SIRENE Bureau on file as a result of exchange of information, will be retained only as long as it is indispensable to attain the objectives for which they were provided. In every case, they shall be deleted no later than one year from the time in which the respective alert has been deleted from the Schengen Information System. The application of the above does not limit the Member State’s right to retain such information in the national files which are related to a certain alert entered by the Member State or to an alert based on which measures have been implemented in its territory. The provisions

concerning the period of retention of such data in the national files are contained in national legislation.

Alerts containing national measures can be retained in the case management system of the SIRENE Bureau for 10 years after they have been deleted from the central system. In order to facilitate the supplementary information, the Member States shall keep in their SIRENE Bureaus the reference data on decisions constituting the basis for the alerts.

Log data shall be deleted within three years from the time in which they have been created. Logs containing the history of alerts shall be deleted within three years from the deletion of the alerts. However, the logs can be kept longer if they are needed for monitoring procedures already underway.

8 Rights of the data subject

To ensure transparent and open provision of information and to promote the exercising of data subjects' rights, the police have made extensive information available to all on the www.poliisi.fi -website. The site offers detailed information on matters such as:

- how a data subject can check his/her personal data
- when the right to check the information can be restricted
- how and on what grounds the information can be rectified or deleted
- how the police process log data
- how the police, in its role as data controller, protects the rights of the data subjects; and
- how internal control is exercised in connection to the processing of personal data.

To ensure that the above-mentioned information is available to all in another manner, as well, a Police Data Files folder can be found at all customer service points of the police. It contains similar information aimed at data subjects in paper format.

8.1 Right of data subjects to check their records / right of access by the data subject

The starting point is that everyone has the right to obtain information from the controller as to whether his/her personal data is processed. If the data is processed, the data subject has the right to obtain from the controller, upon

request, the information specified in section 23 of the Act on Data Protection in Criminal Matters.

When wishing to exercise the right to check the above-mentioned information, the data subject must submit the request to do so to the controller or police department in person and to prove his/her identity. The data subject may bring along an assistant. The request must be sufficiently specific: it must indicate, with sufficient accuracy, which personal data file or part of a personal data file it refers to.

The data subject does not have right of access to personal data of covert human intelligence sources, personal data in the National Schengen Information System relating to discreet checks, inquiry checks and specific checks, information concerning the tactical and technical methods of the police, observation data, personal data of covert human intelligence sources or data used for forensic investigation purposes included in the personal data referred to in sections 5–8 of the Act on the Processing of Personal Data by the Police, or personal data acquired using the intelligence gathering methods in accordance with chapter 5 of the Police Act and chapter 10 of the Coercive Measures Act, or pursuant to section 157 of the Act on Electronic Communication Services.

A data subject's right to check information can be restricted if, taking into consideration the data subject’s rights, it is necessary and proportionate in order to:

1) prevent, uncover or solve crimes, take legal action in connection to a crime or avoid inconvenience in connection to the enforcement of criminal sanctions
2) safeguard investigation, clarification or similar procedures
3) preserve public safety
4) preserve national security or
5) protect the rights of other people.

If a data subject’s right to check information is suspended, restricted or refused, the controller must, without undue delay, inform the data subject of this in writing. The grounds for the suspension, restriction or refusal must also be stated, unless doing so would jeopardize the purpose of the denial or restriction. If the data subject has not, within three months of making the request, received a written reply, this will be considered tantamount to refusing the right of access.

Data subjects have the right to request the Data Protection Ombudsman to investigate the legality of personal data and its processing if the right of access has been postponed, restricted or denied by virtue of the Act on Data Protection in Criminal Matters or other legislation. The request must be submitted in person to the Data Protection Ombudsman, controller (National Police Board) or police department, and the person submitting the request is required to prove their identity.

Data subjects have the right to refer matters to the Data Protection Ombudsman (request for action) if they consider the processing of their personal data to be in violation of the Act on Data Protection in Criminal Matters or other legislation on the processing of personal data.

Office of the Data Protection Ombudsman:
Street address: Lintulahdenkuja 4, 00530 Helsinki
Postal address: P.O. Box 800, 00531 Helsinki
Telephone exchange: 029 566 6700, Fax: 029 566 6735
Email (registry): tietosuoja@om.fi

8.2 Rectification or erasure of personal data and restriction of processing

The controller must, unprompted or at the demand of the relevant data subject and without undue delay, rectify or complete personal data that is inaccurate or incomplete for the purpose of its processing.

The controller must, unprompted or at the demand of the relevant data subject and without undue delay, erase personal data if its processing violates the requirements of the Act on Data Protection in Criminal Matters regarding legality, purpose of use, necessity or accuracy, or the provisions regarding special categories of personal data.

However, instead of erasing the data, the controller must restrict its processing if:
1) the data subject contests the accuracy of the data, and its accuracy or inaccuracy cannot be verified (before removing this restriction, the controller must inform the data subject of the removal) or
2) the personal data has to be retained for evidence purposes.

The data subject can submit the request to have his/her personal data rectified or erased or to have its processing restricted to the controller or another police unit.

The request must be sufficiently specific:
- it must indicate whose personal data it concerns
- which personal data the data subject wishes to have rectified or erased or the processing of which data the data subjects wishes to have restricted
- why the data subject finds the data incomplete, inaccurate or defective for its purpose of processing
- what changes the data subject demands to the data, and
- why the processing of the data should be restricted.

The controller is entitled to request further information to confirm the identity of the data subject.

A data subject's right to have personal data rectified or erased or to have the processing of data restricted can be restricted if, taking into consideration the data subject's rights, it is necessary and proportionate in order to:
1) prevent, uncover or solve crimes, take legal action in connection to a crime or avoid inconvenience in connection to the enforcement of criminal sanctions
2) safeguard investigation, clarification or similar procedures
3) preserve public safety
4) preserve national security or
5) protect the rights of other people.

If the controller refuses the data subject's request to have data rectified, completed or erased or to have the processing of data restricted, the controller must inform the data subject of this refusal and its grounds in writing. The grounds for the refusal can be omitted fully or in part to the extent that this is necessary on the grounds specified in the previous section.

The data subject has the right to request the Data Protection Ombudsman to check the legality of personal data and its processing if, pursuant to the Act on Data Protection in Criminal Matters or some other law, the controller does not accept the data subject's request to have his/her data rectified, completed or erased or to have the processing of this data restricted (contact information provided above).

When inaccurate personal data is rectified, the controller must notify the authority from which the inaccurate data was obtained. If personal data has been rectified or completed or if its processing has been restricted on the basis of section 25 of the Act on Data Protection in Criminal Matters, the controller must notify the

recipients to which it has disclosed this data. The recipients must also rectify or erase this personal data or restrict its processing.

8.3 Other rights of the data subject

The data subject's right to object to the processing of data, right to have the data transmitted from one system to another and right not to be subjected to automated decision-making do not apply when the police processes personal data in connection with a statutory police duty related to the prevention and uncovering of crimes or in order to exercise the official authority of the police.

8.4 The data subject's right to exercise rights and have action taken free of charge

Generally, there is no fee for the notifications and information sent to a data subject on the basis of the Act on Data Protection in Criminal Matters or for the processing of the requests submitted by the data subject. However, if the requests of the data subject are clearly unreasonable or unfounded because of their frequency or for other reasons, the controller may charge a fee. The grounds for the fee amounts are specified in the Act on Criteria for Charges Payable to the State (150/1992). If the controller charges a fee on the above grounds, it must be able to demonstrate that the request is clearly unfounded or unreasonable.

9 Protection and monitoring of personal data by the police

The controller and the processor of personal data must ensure, through technical and organizational measures, that personal data is sufficiently protected, taking into consideration the threats posed to the data subject's rights by the processing. In particular, personal data must be protected from unlawful processing and accidental deletion, destruction and corruption. When planning and implementing measures, the following must be taken into consideration:

1) the latest technology
2) the implementation costs of the measures
3) the nature, extent, context and purposes of processing and
4) the threats posed to the rights of a natural person, which vary in probability and severity.

The basis of the National Police Board's technical, administrative and organizational information security is the information security and protection policy, which defines the goals, responsibilities, implementation measures and

means of implementation in police administration. The information security policy is expanded upon in various separate regulations and guidelines.

The National Police Board has issued a guideline on internal legality control and certain other legal matters in the police. The guideline provides the basis for the planning and realization of internal legality control by the police and the reporting of the results, also in regard to monitoring the use of information systems and the processing of personal data by the police.

In the legality control of the use of personal data files and the processing of personal data, special attention is paid to the accuracy of and need for the processed data, the appropriate use of the data, the correctness and validity of access rights, and the processing of data in accordance with the classification requirements for confidential documents and information. In the monitoring of the processing of special categories of personal data, special attention is paid to appropriate implementation of the technical and organisational protection measures required to safeguard data subjects' rights, as well as to making sure that personal data is only processed when it is necessary for the police to perform its statutory duties.

10 Availability of privacy statements

The privacy statements of the police are publicly available in electronic format on the national police information network (www.poliisi.fi/en) and in the internal information network of the police (Intranet), and in paper format at all customer service points of the police.

In addition, privacy statements are stored in the police's administrative case management, decision-making and archiving system (Acta).