Privacy statement; Processing of personal data in the National subsection of the Schengen information System

POL-2019-22330, ID-20369729, 28.10.2020

1 Controller

National Police Board
Postal address: PO Box 22, FI-00521 Helsinki, Finland
Street address: Asemapäällikönkatu 14, Helsinki
Telephone: +358 295 480 181 (exchange)
E-mail: kirjaamo.poliisihallitus@poliisi.fi

2 Contact person in data protection matters

National Police Board
Päivi Laaksonen
Contact information: See section 1

3 Data Protection Officer of the Police

National Police Board
Harri Kukkola, Senior Adviser
Contact information: 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 with 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.

Provisions 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:

1) Act on the Processing of Personal Data by the Police (616/2019, hereinafter the Police Personal Data Act)

2) 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 legislative instrument of the Schengen Information System.

The legislative instrument of the Schengen Information System means Regulation (EC) No 1987/2006 of the European Parliament and of the Council on the establishment, operation and use of the second generation Schengen Information System (SIS II), Council Decision 2007/533/JHA on the establishment, operation and use of the second generation Schengen Information System (SIS II) and Regulation (EC) No 1986/2006 of the European Parliament and of the Council regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates, and the Schengen acquis as referred to in Article 1(2) of Council Decision 1999/435/EC of 20 May 1999 (hereinafter the Convention).

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

5.1 Purposes of processing

According to Regulation (EC) No 1987/2006, the purpose of the Schengen Information System is to ensure a high level of security within the area of freedom, security and justice of the European Union, including the maintenance of public security and public policy and the safeguarding of security in the territories of the Member States, and to apply the provisions relating to the movement of persons in their territories, using information communicated via this system.

The Schengen Information System contains alerts for the purpose of refusing entry or stay of third-country nationals. The data may not be used for administrative purposes. However, the right to access data entered in the Schengen Information System and the right to search such data directly may also be exercised by national judicial authorities, including those responsible for the initiation of public prosecutions in criminal proceedings and for judicial inquiries prior to charge, in the performance of their tasks, as provided for in national legislation, and by their coordinating authorities.

5.2 The categories of data and categories of personal data of the Schengen Information System processed through the user interface of the National subsection of the Schengen Information System are presented in the chapters below.

- Regulation (EC) No 1987/2006 defines that the alerts issued in respect of third-country nationals for the purpose of refusing entry and stay and the information on persons in relation to whom an alert has been issued shall be no more than the following:
  a) surname(s) and forename(s), name(s) at birth and previously used names and any aliases which may be entered separately
  b) any specific, objective, physical characteristics not subject to change
  c) place and date of birth
  d) sex
  e) photographs
  f) fingerprints
  g) nationality(ies)
  h) whether the person concerned is armed, violent or has escaped
  i) reason for the alert
  j) authority issuing the alert
  k) a reference to the decision giving rise to the alert
  l) action to be taken
  m) link(s) to other alerts issued in SIS II in accordance with Article 37.

Additionally, the following alert purposes are defined in Council Decision 2007/533/JHA:

- alerts in respect of persons wanted for arrest for surrender or extradition purposes
- alerts on missing persons
- alerts on persons sought to assist with a judicial procedure
- alerts on persons and objects for discreet checks or specific checks
- alerts on objects for seizure or use as evidence in criminal proceedings.

For the alert purposes set out in Council Decision 2007/533/JHA - excluding, however, the provisions pertaining to the exchange of supplementary information and storage of additional data - the information on persons in relation to whom an alert has been issued shall be no more than the following:

a) surname(s) and forename(s), name(s) at birth and previously used names and any aliases which may be entered separately

b) any specific, objective, physical characteristics not subject to change
c) place and date of birth
d) sex
e) photographs
f) fingerprints
g) nationality(ies)
h) whether the person concerned is armed, violent or has escaped
i) reason for the alert
j) authority issuing the alert
k) a reference to the decision giving rise to the alert
l) action to be taken
m) link(s) to other alerts issued in SIS II pursuant to Article 52
n) the type of offence.

Additionally, the following provisions are set out in the Council Decision on alerts issued for a different purpose:

- Alerts in respect of persons wanted for arrest for surrender or extradition purposes (Article 26)
  - the issuing Member State shall enter in SIS II a copy of the original European Arrest Warrant
  - The Member State which entered the alert in SIS II for arrest for surrender purposes shall communicate the information referred to all Member States through the exchange of supplementary information.

- Alerts on missing persons who need to be placed under protection and/or whose whereabouts need to be ascertained (Article 32). The following categories of missing persons may be entered:
  a) missing persons who need to be placed under protection for their own protection or in order to prevent threats
  b) missing persons who do not need to be placed under protection.

- Alerts on persons sought to assist with a judicial procedure (Article 34). For the purposes of communicating their place of residence or domicile Member States shall, at the request of a competent authority, enter in SIS II 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 deprivation of liberty.

- Alerts on persons and objects for discreet checks or specific checks. Data on persons or vehicles, boats, aircrafts and containers shall be entered in accordance with the national law of the Member State issuing the alert, for the purposes of discreet checks or specific checks in accordance with Article 37, paragraph 4 (Article 36). Alerts on vehicles, boats, aircrafts and containers may be issued where there is a clear indication that they are connected with the serious criminal offences or serious threats. Such an alert may be issued for the purposes of prosecuting criminal offences and for the prevention of threats to public security:
  a) where there is clear indication that a person intends to commit or is committing a serious criminal offence or
  b) where an overall assessment of a person, in particular on the basis of past criminal offences, gives reason to suppose that that person will also commit serious criminal offences in the future.

For the purposes of discreet checks or specific checks, all or some of the following information shall be collected and communicated to the authority issuing the alert when border control or other police and customs checks are carried out within a Member State:

a) the fact that the person for whom, or the vehicle, boat, aircraft or container, for which an alert has been issued, has been located
b) the place, time or reason for the check
c) the route and destination of the journey
d) the persons accompanying the persons concerned or the occupants of the vehicle, boat or aircraft who can reasonably be expected to be associated to the persons concerned
e) the vehicle, boat, aircraft or container used
f) objects carried

g) the circumstances under which the person or the vehicle, boat, aircraft or container was located.

- The following categories of readily identifiable objects shall be collected and entered in alerts on objects for seizure or use as evidence in criminal proceedings (Article 38):
  a) motor vehicles with a cylinder capacity exceeding 50cc, boats and aircrafts
  b) trailers with an unladen weight exceeding 750 kg, caravans, industrial equipment, outboard engines and containers
  c) firearms
  d) blank official documents which have been stolen, misappropriated or lost
  e) issued identity papers such as passports, identity cards, driving licenses, residence permits and travel documents which have been stolen, misappropriated, lost or invalidated
  f) vehicle registration certificates and vehicle number plates which have been stolen, misappropriated, lost or invalidated
  g) banknotes (registered notes)
  h) securities and means of payment such as cheques, credit cards, bonds, stocks and shares which have been stolen, misappropriated, lost or invalidated.

- Data relating to a person whose identity has been misused shall be used only for the following purposes:
  - to allow the competent authority to distinguish the person whose identity has been misused from the person actually intended as the subject of the alert
  - to allow the person whose identity has been misused to prove their identity and to establish that their identity has been misused.

6 Regular disclosure of data

6.1 Disclosure of personal data from the National subsection of the Schengen Information System

The police may, non-disclosure provisions notwithstanding, disclose data from the National Schengen Information System to the competent Schengen authorities in compliance with the provisions set out in the legislative instrument of the Schengen Information System. Data may also be disclosed by means of a technical operating connection, or as a set of data.

6.2 Disclosure of personal data to a state using the Schengen Information System and to the Schengen Information System

The police may, non-disclosure provisions notwithstanding, disclose to competent Schengen authorities and for retention in the Schengen Information System any data referred to in the legislative instrument of the Schengen Information System which is necessary for the purposes set out in the legislative instrument of the Schengen Information System. Supplementary information referred to in the legislative instrument of the Schengen Information System must be disclosed via the SIRENE Bureau. The National Bureau of Investigation serves as the SIRENE Bureau in Finland. Data may also be disclosed by means of a technical operating connection, or as a set of data.

7 Erasing and archiving of personal data

The legislative instrument of the Schengen Information System sets out the following provisions on the erasure of personal data:

- Alerts entered in SIS II pursuant to Regulation (EC) No 1987/2006 shall be kept only for the time required to achieve the purposes for which they were entered. A Member State issuing an alert shall, within three years of the alert's entry, review the need to keep it. Within the review period, a Member State issuing an alert may, following a comprehensive individual assessment, decide to keep the alert longer, should this prove necessary for the purposes for which the alert was issued. Each Member State shall, where appropriate, set shorter review periods in accordance with its national legislation.
- Alerts on persons entered in SIS II pursuant to Decision 2007/533/JHA shall be kept only for the time required to achieve the purposes for which they were entered. A Member State issuing an alert shall, within three years of the alert's entry, review the need to keep it. However, the period shall be one year in the case of alerts on persons referred to in Article 36. Within the review period, a Member State issuing an alert may, following a comprehensive individual assessment, decide to keep the alert longer, should this prove necessary for the purposes for which the alert was issued.
- Alerts on objects entered in SIS II pursuant to Decision 2007/533/JHA shall be kept only for the time required to achieve the purposes for which they were entered. Alerts on objects entered in accordance with Article 36 shall be kept for a maximum of five years, and data retained on objects entered in accordance with Article 38 shall be kept for a maximum of 10 years, with the exception of alerts on means of payment, the period of validity of which is one

year. The retention periods referred to above may be extended should this prove necessary for the purposes for which the alert was issued.

- Additional data for the purpose of dealing with misused identity shall be erased at the same time as the corresponding alert or earlier if the person so requests.
- Personal data held in files by the SIRENE Bureau as a result of information exchanged shall be kept only for the time required to achieve the purposes for which the data was supplied. The data shall, in any event and at the latest, be deleted one year after the related alert has been deleted from SIS II.
- Log records shall be erased one to three years after they were created. Records which include the history of alerts shall be erased one to three years after deletion of the alerts. However, records may be kept longer if they are required for monitoring procedures that are already under way.

8 Rights of the data subject

For the sake of transparency and openness of information and for facilitating the exercise of the rights of the data subject, the police has made comprehensive information material available for all on the www.poliisi.fi website. The site contains detailed information about how a data subject may access the data pertaining to them, when the right of access can be limited, how and under which conditions the data may be corrected or erased, how the log data are processed by the police, and how the police as the data controller ensures the rights of the data subject and the internal control of 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

According to the legislative instrument of the Schengen Information System, the right of persons to have access to data relating to them entered in SIS II shall be exercised in accordance with the law of the Member State before which they invoke that right. According to the legislative instrument, information shall not be communicated to the data subject if this is indispensable for the performance of a lawful task in connection with an alert or for the protection of the rights and freedoms of third parties.

As a rule, everyone has the right to obtain information from the data controller as to whether their personal data are being processed. If the data is processed, the data subject has the right to obtain from the controller, upon request, the information set out in section 23 of the Act on Data Protection in Criminal Matters.

In order to exercise their right of access with regard to said data, the data subject must make a request to this effect personally to the data controller or at a police department and prove his identity. The data subject may bring along an attorney. The request must be specified to a sufficient accuracy level of detail to indicate which personal data file or part of a personal data file it refers to.

According to the legislative instrument of the Schengen Information System, the individual concerned shall be informed as soon as possible and in any event not later than 60 days from the date on which they apply for access or sooner, if national law so provides.

The data subject has no right of access to informant data, personal data in the Schengen Information System concerning discreet surveillance or specific checks, data concerning tactical and technical methods of the police included in the personal data referred to in sections 5 through 8 of the Act on the Processing of Personal Data by the Police, observation or informant data or information used for forensic investigation, or personal data obtained using information gathering methods pursuant to chapter 5 of the Police Act and chapter 10 of the Coercive Measures Act and under section 157 of the Information Society Code.

The right of access of the data subject may be restricted if this, considering the rights of the data subject, is proportionate and necessary in order to:

1) avoid detriment to the prevention, detection, investigation or prosecution of criminal offences or the enforcement of criminal sanctions
2) safeguard any other investigation, examination or other procedure of an authority
3) protect public security
4) protect national security or
5) protect the rights of other persons.

If the right of access of the data subject is postponed, restricted or refused, the data controller shall, without undue delay, inform the data subject thereof by a written certificate. The grounds for the postponement, restriction and refusal shall

also be stated, unless this would undermine the purpose of the refusal or restriction. The data controller is also considered to have refused the right of access if the data controller, within three months after the making of the request, has not replied to the data subject in writing.

The data subject has the right to request the Data Protection Ombudsman to verify the lawfulness of the personal data and their processing if the right of access of the data subject has been postponed, restricted or refused by virtue of the Act on Data Protection in Criminal Matters or another Act. The request must be made in person to the Data Protection Ombudsman, the data controller (National Police Board) or the police department concerned, and the individual making the request is required to prove their identity.

If a data subject considers that the Act on Data Protection in Criminal Matters or another Act concerning the processing of personal data is being infringed in the processing of their personal data, they have the right to refer the matter to the Data Protection Ombudsman (request for measures).

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, erasure and restriction of processing of personal data

According to the legislative instrument of the Schengen Information System, any person has the right to have any factually inaccurate data stored in SIS II relating to them corrected, or unlawfully stored data relating to them deleted. According to the legislative instrument, the individual shall be informed about the follow-up performed on the exercise of their rights of correction and deletion as soon as possible and, in any event, no later than three months from the date on which they apply for correction or deletion, or sooner if national law so provides.

The data controller shall, on its own initiative or at the request of the data subject, without undue delay, rectify or supplement any personal data concerning the data subject if they are incorrect or incomplete for the purpose of the processing.

The controller shall, spontaneously or at the request of the data subject, without undue delay, erase any personal data of the data subject if their processing

conflicts with the provisions of the requirement of lawfulness, purpose limitation, requirement of necessity, requirement of accuracy or processing of special categories of personal data.

Instead of erasing the data, the controller shall, however, restrict the processing if:

1) the data subject contests the accuracy of the data and their accuracy or inaccuracy cannot be ascertained (the controller shall inform the data subject of this before lifting this restriction) or
2) the data must be maintained for the purposes of evidence.

The data subject may submit a request for rectification, erasure or restriction of processing of personal data with the data controller or other 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 data 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 data controller refuses the request of the data subject to rectify, supplement or erase personal data or to restrict their processing, the data controller shall inform the data subject of the refusal and its grounds by a written certificate. The information on the grounds for the refusal may be omitted wholly or partly to the extent that this is necessary on the grounds mentioned above.

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.

The data controller shall communicate any rectification of inaccurate personal data to the authority from which the inaccurate personal data originate. If personal data have been rectified or erased or if their processing has been restricted by virtue of section 25 of the Act on Data Protection in Criminal Matters, the data controller shall communicate the matter to the recipients to whom the data controller has disclosed such data. The recipient shall rectify or erase any such personal data possessed by it or restrict their processing.

According to the Police Personal Data Act the data that have been found to be erroneous may be retained alongside corrected data if this is necessary for safeguarding the rights of the data subject, another party involved or police personnel. However, no data that have been found to be erroneous may be retained in the National subsection of the Schengen Information System.

8.3 Other rights of the data subject

The data subject's right to object to the processing of the data, right to data portability and right not to be the subject of automated decision-making shall not be applied when the personal data are being processed by the police in connection with its statutory duty related to the prevention or detection of criminal offences and to exercise the public authority vested with the police.

Everyone has the right to ask the supervisory authority referred to in the Schengen Convention to verify that the collection, recording, processing and utilisation 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. The data subject must make a request to this effect personally to the controller or at a police department and prove their identity. Any verification request presented to the police shall be forwarded to the Data Protection Ombudsman without delay.

8.4 Exercise of the rights of the data subject and provision of measures free of charge

As a rule, the communications and information given to the data subject and the consideration of the requests made by the data subject in accordance with the Act on Data Protection in Criminal Matters are free of charge to the data subject. However, if the requests of the data subject are manifestly unreasonable or unfounded because of their recurrence or for another reason, the controller may collect a charge for the measure. Provisions on the criteria for the charges are laid down in the Act on Criteria for Charges Payable to the State (150/1992). If the controller collects a charge on the aforementioned grounds, it shall, where necessary, demonstrate that the request is manifestly unfounded or unreasonable.

9 Protection and control of personal data by the police

The data controller and the processor shall, by technical and organisational measures, ensure an adequate protection of the personal data, taking into account the risk resulting from the processing to the rights of the data subject. In particular, the personal data shall be protected against unlawful processing and accidental loss, destruction and damage. In planning and implementing the measures, account shall be taken of:

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.

Technical, administrative and organisational information security within the police administration is based on the Police’s information security and data protection policy that lays down the objectives of information security as well as the associated division of responsibilities and procedures within the police administration. A number of separate regulations and guidelines will be issued to specify the information security policy in more detail.

The National Police Board has issued a guideline on internal legality control and certain legal matters in the police which provides a framework for the planning and implementation of the police’s legality control and for reporting on the results also with regard to the oversight of the use of the information systems of the police and the processing of personal data.

In the legality control of the use of personal data files and the processing of personal data, special attention shall be paid to the correctness of, and need for, the data being processed, the appropriate use of the data, the correctness and validity of access rights, and that the data are processed in accordance with the classification requirements for secret documents and information. In the control of the processing of personal data belonging to special categories of personal data, special attention shall be paid in ensuring that the technical and organisational security measures required for safeguarding the rights of the data subjects have been appropriately implemented and that the personal data concerned are only processed when necessary for the discharge of the duties imposed upon the police by law.

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.

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