

The Police Data Protection Policy

The police have the role according to law to guard the public safety and to ensure legal protection, stem the commission of crimes and to work toward the disclosure of crimes, give assistance to the citizens and to assist the authorities in the execution of their work, and to enforce the public peace and public order. The processing of personal data is therefore a necessary component of police work. The police places heavy emphasis on the protection of personal data and that the processing of such data is compliant with the provisions of the data protection act.

The objective of the data protection policy is to provide information on how the police processes personal data, for which purpose, and how the data is used. This policy applies to individual persons but not to legal entities.

Personal data are any kind of information about a personally identified or a personally identifiable individual, i.e. information which can be traced directly or indirectly to a specific individual.

Controller

The National Commissioner of the Icelandic Police, Skúlagata 21, 101 Reykjavík, oversees police matters as commissioned by the Minister – the country is divided into nine police districts.

- Police Commissioner of Reykjavík Capital area, Hverfisgata 113, 105 Reykjavík.
- Police Commissioner of Vesturland, Bjarnabraut 2, 310 Borgarnes.

- Police Commissioner of Vestfirðir, Hafnarstræti 1, 400 Ísafjörður.
- Police Commissioner of Norðurland vestra, Suðurgata 1, 550 Sauðárkrókur.
- Police Commissioner of Norðurland eystra, Þórunnarstræti 138, 600 Akureyri.
- Police Commissioner of Austurland, Strandgata 52, 735 Eskifjörður.
- Police Commissioner of Suðurland, Hlíðarvegur 16, 860 Hvolsvöllur.
- Police Commissioner of Suðurnes, Brekkustígur 39, 230 Reykjanesbær.
- Police Commissioner of Vestmannaeyjar, Faxastígur 42, 900 Vestmannaeyjar.

Further information about the agencies is posted here on the police website (under “police” in the menu). The National Commissioner keeps the police records according to the Police Act, this means that the Commissioner is responsible for the operation and security of the records. Each agency by itself is the responsible party for the processing of personal data by its staff, i.e. what they enter into the systems on each occasion. In some instances the agencies may be considered to be jointly responsible parties.

What processing of personal data is conducted by the police, for what purpose and based on which authority?

The police and their function are governed by the Police Act No. 90/1966. In addition, the police are also commissioned to enforce various acts of law, e.g. the Criminal Code, the Firearms Act and the Traffic Code to name a few. Provisions on investigation and criminal prosecution are found in the code of criminal procedure and in regulations enacted in accordance with that code. Furthermore, these procedures are supported by instructions issued by the office of the Director of Public Prosecutions who is the supreme occupant of the office of the public prosecutions.

The police gather information from various entities in their execution of their statutory tasks in connection with the purpose of preventing, investigating, detecting, or prosecuting punishable offences, including to protect against and to prevent threats, and this processing is subject to Act No. 75/2019 on the processing of personal data for law enforcement purposes. Special regulations on the handling of personal data for the Schengen Information Systems are listed in Act No. 16/2000. All other processing by the agencies of personal data that relates to the public administration, operations, personnel administration, procurement etc., is subject to Act No. 90/2018 on Data Protection and the processing of personal data, and to the European Parliament and Council regulation (EU) 2016/679 as enacted into law in Iceland.

Data used in police work may contain general information and sensitive information such as e.g.

- Contact details / Communications information such as name, ID number, address, nationality-citizenship, telephone number and e-mail address.
- information about an offence, scene, and fine amount
- information about occupation and education
- financial information
- information about race and ethnical background
- information about physical characteristics, such as fingerprints and DNA sample,
- photos, audio recordings and video recordings.
- criminal record certificate
- information about an accident
- information about mental and physical health
- electronic monitoring, i.a. at police stations
- IP numbers

The police endeavour to only record and preserve that information to the degree necessary

Access to the police docket

The police staff only have access to the information that they need in order to perform their work, and it depends on the field of work of each person which information the staff member has access to

Confidentiality

All members of the staff are bound under law by professional secrecy, which continues even when the person retires. The professional secrecy of the police staff is governed by, in particular, the provisions of Art. 18 of Act on the Rights and Obligations of Government Employees, the provisions of Chapter X of the Administrative Procedures Act, as well as par. 4 of Art. 18 of the Act on Criminal Procedures, and Art. 22 of the Police Act. Furthermore, the police staff must abide by the police Ethics Code in all respects.

The staff take care that all personal data is managed as confidential matter and all employees sign a confidentiality statement. If the processing of personal information is to some extent being handled by third party, then those employees of the third party who have access to the information also sign a confidentiality agreement.

Retention period

Personal data is preserved while it is needed and there are objective reasons for this, or as stipulated by law if the retention period is stated in the law. The police are subject to surrender requirements according to the Act on public archives, and they may therefore not dispose of, or destroy any document that comes under the purview of the act, except with the permission of the state archivist.

From where does the personal data come and where to is it disseminated?

The processing of personal data is a prerequisite that the police can perform its role. Personal data arrive from and this is not an exhaustive list of individuals, and their representatives, institutions, other competent authorities, international law enforcement agencies, courts and prisons.

To whom is personal data disseminated?

The police may deliver personal data to a third party based on a legal requirement that is incumbent upon the police. An example of this is the return of documents to the state archive of Iceland, a defence counsel, courts of justice, tax authorities or e.g. other authorities, individuals or legal persons who demonstrate a right to such information, or who have legally protected interests in getting such information, provided the delivery is in accordance with applicable law.

It may also be necessary to share information with other competent authorities, across this country and in the international arena, with partner institutions in order to reduce crime and to prevent international criminal activity.

In some instances the police may apply a processing party who has entered into a contract with the police about the processing of personal information.

Rights of a registered person

An individual may request to receive information about the processing of own personal data by the police and may also request access to this data. There are however various limitations regarding the access to data and information according to the act on criminal procedure, the administrative procedures act and the data protection act. Each such

request is assessed and a decision is taken about which information will be provided and how access to that information will be arranged.

With reservations regarding the preconditions in the data protection act, individual persons have in some instances a right to get information corrected, or to request a limitation on the processing.

Requests can be directed to the e-mail address personuvernd@logreglan.is and sudurnes.personuvernd@logreglan.is (for requests to the police commissioner of Suðurnes).

An individual is at the same time entitled to lodge a complaint to the Data Protection Authority which has a supervisory role in the field of data protection, see website of the agency: www.personuvernd.is

The security of personal data

The police attach great significance to ensuring the safety of the users personal data. The police computer and information systems are operated in a closed-circuit wide area network and hosted at the National Commissioner of the Icelandic Police. The police endeavours to resort to the proper technical and organisational measures in order to protect personal data, taking into consideration their nature.

Examples of such security measures are access control for systems, function recording in order to ensure the traceability of actions, multi-layered identification, encryption of data and transmissions and regular updates and instructions for users.

Data protection representative

The Data protection representative has supervision of the applicable laws and regulations about data protection are followed by the police. Enquiries, commentaries, and suggestions that relate to data protection can be directed to the data protection representative.

Enquiries and comments

You can contact the data protection representative at the National Commissioner of the Icelandic Police, with the exception of the police commissioner of Suðurnes, by calling telephone No. 444-2500 or by sending an e-mail to the e-mail address personuvernd@logreglan.is. It is also possible to send a hard-copy letter to the National Commissioner of the Icelandic police: Ríkislögreglustjóri, Skúlagata 21, 101 Reykjavík, but in that case the envelope must be marked Data Protection Representative.

You can contact the data protection representative of the police commissioner in Suðurnes by calling phone number 444-2200, or by sending an e-mail to the e-mail address sudurnespersonuvernd@logreglan.is. It is also possible to send a hard-copy letter to the police commissioner in Suðurnes, Hringbraut 130, Reykjanesbær, but in that case the envelope must be marked Data Protection Representative.

Police on Facebook

The police uses facebook in order to facilitate dissemination of information to the public. If a person chooses to deliver a formal message to the police or to share information relating to the investigation of a criminal case, the police wishes to emphasize that such information must be formally delivered to the police by a telephone call to 112, or to the relevant agency, by regular mail, by e-mail or by the use of a police website button.

If an individual uses the police Facebook page in order to send a message to the police it is important to keep in mind that this information is also shared with Facebook.

A change in the Police Data Protection policy

The police will work on the continued development and improvement of the work procedures regarding the handling of personal data. The police will revise this policy on a regular basis as may be necessary.

Approved at the meeting of the Police Council

15. April 2021