Whistleblowing – notification channel register

Updated
29.06.2023

Privacy statement

Registrar

Suomen Kaukokiito Oy (0114330-2)
Teollisuustie 7
Tampere
33330
0105100

Contact person in matters concerning the register

tietosuoja@kaukokiito.fi

Draft date

22.2.2023

Legal basis for processing

EU directive 2019/1937
Law on the protection of persons reporting violations of European Union and national law 1171/2022

Based on the content of the notice, the legal basis is either:
- a legal obligation (reported information under the directive) or
- legitimate interest (declared information outside the directive)
The processing of the data is based on the legitimate interest and on the so-called “Whistleblower Directive” and are processed to investigate and prevent abuses, crimes and the like

Basis of legitimate interest

Through the Whistleblowing channel, all employees of the group and also external stakeholders can anonymously report suspected misconduct. Personal data is processed in the investigation of the reported case and in the assessment and implementation of possible sanctions.

Making intentional false statements is prohibited and may result in legal sanctions.

The controller protects privacy and processes personal data collected through the whistleblowing channel in accordance with data protection legislation and good data protection practices.

The personal data groups in question

The name of the person to be notified and other information related to the activity of the person to be notified, as well as the name of the notifier, if the notification has not been made anonymously.

Processing may involve a high risk due to the information provided. The risks have been assessed in more detail in the impact assessment of the notification channel register, which can be found in the “impact assessments” section in the Easy GDPR service.

Recipients and recipient groups

The data controller's and/or the company's own personnel who are the subject of the processing, as well as the subject of the processing and, if a deeper investigation is required, a dedicated outsourcing partner whose GDPR readiness has been checked and with whom other measures in accordance with Article 28 have been taken.

Information can also be disclosed to the police or other authorities in a situation where a crime has occurred or is suspected to have occurred.

Consent

Processing is based on the legitimate interest, so consent is not required.

Data content of the register

The register contains the following information:
- Name of the notifier
- Name of the object of the notification
- Information provided by the notifier that is the subject of the notification.

Personal information that is clearly irrelevant to the processing of a particular notice is not collected, or if it is collected accidentally, it is deleted without undue delay.

Regular sources of information

The data in the register is provided by data subjects (notifiers) themselves.

Personal data retention period

The data in the personal register is kept as long as it is necessary for the controller's possible innocence certificate, but no more than two (2) years after the end of the investigation. The retention period may vary in accordance with mandatory legal requirements, such as criminal procedure and occupational safety laws.

Regular transfers of information

As a rule, the information in the register is not disclosed to third parties, except in deeper investigation situations to selected, GDPR-eligible operators with whom the measures in accordance with Article 28 have been implemented. The information is handed over to the Whistleblowing handler of the company that is the subject of the notification for investigation and for giving a response.

Data transfer outside the EU or EEA

Personal data will not be transferred or processed outside the EU or the EEA.

The service provider outside the Whistleblowing channel uses subcontractors that provide technical data processing services, some of which are located outside the EU in the United States. Kaukokiito has ensured the implementation of appropriate protection measures outside the EU or the EEA by contractual means, ensuring the implementation of an adequate level of data security and compliance with the requirements of legislation concerning the processing of personal data, and by requiring the service provider to use standard clauses established by the European Commission in accordance with Article 46 (2) (c) of the General Data Protection Regulation in its subcontracts for the transfer of personal data.

The latest versions of the standard contractual clauses can be found on the European Commission's website.

Principles of registry protection A: Manual material

The material related to the notification channel register is mainly only in electronic form and the data is processed and stored electronically. Access to the Register's data is only available to those and to the extent required for handling, monitoring or other matters related to the notification.

The data in the register is safeguarded and processed in accordance with the provisions and principles of the Data Protection Act, instructions of the authorities and good data processing practices.

Principles of register protection B: Electronic material

Access to the Register's data is only available to those and to the extent required for handling, monitoring or other matters related to the notification.

The register is stored on a secure server located in Finland.

The data in the register is safeguarded and processed in accordance with the provisions and principles of the Data Protection Act, instructions of the authorities and good data processing practices.

Automatic processing and profiling

Automatic decision-making or other evaluations of persons are not carried out with the monitoring, and the registered person is not harmed or affected by the monitoring.

Inspection right, i.e. the right to get access to personal data

The registered person who is the subject of the notification does not have the right to inspect the information if providing the information could hinder the investigation of suspected violations.

If a telephone line or other voice message system that does not record the conversation is used for notification, the controller has the right to document the oral notification in the form of an accurate protocol written by the staff member responsible for processing the notification. The reporting person then has the opportunity to check, correct and approve the minutes prepared from the discussion with their signature.

The right to transfer data from one system to another

The registered person who is the subject of the notification does not have the right to inspect the information if providing the information could hinder the investigation of suspected violations.

The right to demand correction of information

The reporting person has the opportunity to check, correct and approve the minutes prepared from the discussion with their signature, for example.

The correction request can also be denied. The person responsible for the register provides a written certificate of the refusal to rectify the data, which states the reasons for the refusal. The party concerned may refer the refusal to the data protection ombudsman for a decision.

Right of limitation

The registered person has the right to request the restriction of data processing if, for example, the personal data in the register is incorrect, as long as it does not hinder the investigation of suspected violations or jeopardize the protection of the informant. In this case, the processing is limited until the controller has ensured the accuracy of the data

Right to object

The registered persons do not have the right to object to the processing if it could hinder the investigation of suspected violations or if it would potentially endanger the protection of the informant.

The right to file a complaint with the supervisory authority

If the registered person considers that the data protection regulation has been violated in the processing of personal data concerning them, the registered person has the right to file a complaint with the supervisory authority. The complaint can also be made in the member state where the registered person has a permanent residence or place of employment.
Contact details of the national supervisory authority:

Office of the Data Protection Ombudsman
PO Box 800, Ratapihantie 9,
00521 Helsinki
tel. +358 (0)29 56 66700
tietosuoja@om.fi
www.tietosuoja.fi/en/

Other rights related to the processing of personal data

The registered person has the right to prohibit the disclosure and processing of their data for direct advertising and other marketing, to demand the anonymization of the data where applicable, and the right to be completely forgotten after the end of the employment relationship, unless this could hinder the investigation of suspected violations or possibly endanger the protection of whistleblowers.