PRIVACY NOTICE

EU General Data Protection Regulation (2016/679), Articles 12-14

Date: 29.4.2025, v3

Aidian Oy is committed to protecting privacy and processing personal data in accordance with applicable data protection legislation and good data protection practices. This privacy notice describes how Aidian collects, processes and protects the personal data of the person who has made a report of suspected misconduct (the so-called whistleblowing report) (the 'reporter') and the personal data of the person who is the subject of the whistleblowing report (the 'reported'). The report can be submitted anonymously, but it is possible that the identity of the reporter of an anonymous report may also appear indirectly from the information provided by the reporter in the report. However, Aidian does not attempt to identify the reporter unless it is absolutely necessary for the investigation of the matter.

We may update or change this privacy notice at any time and, if required by law, we will notify the data subjects thereof.

1. Controller and/or joint controller	Aidian Oy Koivu-Mankkaan tie 6B 02200 Espoo Finland Tel. +358 10 309 300 Business ID: 1855216-1
2. Contact details for data protection matters	**Data Protection Officer:** E-mail address: dataprotection@aidian.eu Telephone: 010 309 3000 (center) Postal address: Aidian Oy / Data protection issues, Koivu-Mankkaan tie 6B, 02200 Espoo
3. Name of the register	Aidian's whistleblowing channel and the process for solving the whistleblowing reports
4. Purpose of the processing of personal data and legal basis for the processing of personal data	**Purpose of the processing of personal data:** Personal data is processed in relation to whistleblowing report processing. The report may be submitted anonymously. However, it is possible that the identity of the reporter may be indirectly revealed from the information provided in the report. In addition, the reporter may provide personal information about the person who is the subject of report. The purpose of the whistleblowing channel is to enable the reporting of observed or suspected activity against the public interest or ethical principles in connection with work. **Legal basis for the processing of personal data:** Personal data is processed to comply with the controller's legal obligation (GDPR Article 6(1)(c) and for an important public interest reason: processing reports of suspected misconduct (GDPR Article 9(2)(g). The obligation is based on European Union Directive 2019/1937 and the resulting national legislation, whistleblower protection act 1171/2022.

5. Data contained in the register	It is possible to report anonymously or under your own name. The report is always treated confidentially, and the identity of the reporter is known only to the persons appointed to process the reports and to the persons invited to investigate the report as substance matter experts. The register may contain the following types of personal information concerning the reporter and the reported, as well as other persons related to the matter, such as witnesses: • Name, e-mail address and phone number of the reporter. The report can also be made totally anonymously. • Information in the report, including the name of the reported, information related to possible illegal activity (incl. place and time), witness information. Information related to making and processing the report as well as messages (including notification code and status). • Any other information provided by the reporter. The information may contain special categories of personal data (e.g. information about the person's health condition), or criminal or violation information to the extent that these come up in the investigation process. The instructions of the Whistleblowing channel advice the reporter to limit reported personal data to only necessary and appropriate, but since the reporters can enter the data themselves, the data controller does not have the possibility to restrict what personal data is entered into the report. Therefore, it is possible that special categories of personal data are also processed.
6. Data sources	The primary data source for the information stored in the register is the reporter itself, i.e. the whistleblowing report. In addition, the data may consist of information stored in the process of handling whistleblowing reports, such as information obtained from potentially related persons and information from IT systems.
7. Disclosure of data and parties data are disclosed to, data transfers outside EU/EEA area	The identity of the reporter, when it is known, will not be disclosed to the persons against whom the claims are directed. The identity of the reporter will only be disclosed if authorised by the reporter or if required in criminal proceedings. Personal data is disclosed to third parties, such as authorities or external inspectors, only when necessary. The system provider of the whistleblowing channel used by Aidian is Juuriharja Consulting Group Oy and its subprocessor Gofore Oyj, who may have access to information in emergency or error situations where technical support is required. The whistleblowing channel is implemented as a cloud service and the data is stored in the EU/EEA area. Personal data is primarily not transferred outside the EU or EEA. In exceptional situations, data transfer outside the EEA takes place using the Commission's standard contractual clauses and implementing other appropriate protective measures (e.g. the data is in encrypted form). Direct identifiers such as name or contact information are also not mainly collected (unless the reporter decides to provide them themself in connection with the notification).
8. Retention period of personal data	The report and any supporting documents will be retained for 5 years from the receipt of the report, unless further actions essentially related to the matter are in progress or longer storage is necessary to prepare, present or defend a legal claim.

	If some personal information is not necessary for processing the report or otherwise in the investigation process, it will be removed from the investigational material earlier without undue delay.
9. Principles of the register's security measures	Aidian has implemented appropriate technical and organizational measures to protect personal data from accidental or unlawful loss, disclosure, misuse, alteration, destruction or unauthorized access. The personal data in the whistleblowing channel and in the investigation process are handled confidentially and only in a secure environment designated for this purpose. Personal data can only be accessed by those designated independent members of the Whistleblow team who need to receive the information in order to carry out the investigation or implement possible sanctions. **Principles of whistleblowing channel protection:** The whistleblowing channel is protected by technical means (encryption techniques, firewalls). The whistleblowing channel does not store IP addresses or other such information that could identify the reporter of the notification. The information security of the whistleblowing channel has been verified by an external auditor and it meets the regulatory requirements set for it. The data in the system is regularly backed up. The system does not store any information about the person making the report which they do not themselves report there. During the reporting phase, the reporter receives a number code that allows them to log in and monitor the processing of the report after the report is made. This number code given when making the report is the only way to access the report afterwards. For this reason, the reporter should save the number code for themselves, because this unique number code is the only way to monitor the processing of the notification or provide additional information to the notification. If the number code is forgotten, the notifier has to make a new notification. Only independent persons specifically designated by Aidian are entitled to process reports received through the notification channel.

10. Data subject's rights	The rights of the data subject vary according to the legal basis of the processing.
	
	The data subject can exercise the rights mentioned below by contacting the controller using the contact information specified in section 2, preferably by e-mail.
	
	When the legal basis for the processing is a legal obligation, the data subject has the following rights:
	• The right to receive information about the processing of personal data.
	• The right to access personal data.
	  ○ The data subject has the right to receive confirmation from the controller as to whether personal data concerning them is being processed. The data subject also has the right to get access to the personal data concerning themselves and to information about the processing of their personal data.
	• The right to rectification of data.
	  ○ The data subject has the right to have inaccurate and incorrect personal data concerning them be rectified without undue delay and incomplete personal data to completed.
	• The right to restrict processing.

	○ In certain situations, the data subject has the right to demand that the controller restricts the processing. • The data subject has the right not to be subject to a decision that is based solely on automatic processing, such as profiling, and that has legal effects concerning them or that significantly affects them in a similar way. • The right to file a complaint with the supervisory authority. ○ The data subject has the right to file a complaint with the supervisory authorities if the data subject considers that their rights have been violated in the light of the EU data protection regulation: Office of the Data Protection Ombudsman www.tietosuoja.fi/yhteystiedot Visiting address: Lintulahdenkuja 4, 00530 Helsinki Postal address: PL 800, 00531 Helsinki Switchboard.: 029 566 6700 Registry: 029 566 6768 E-mail (registry): tietosuoja(at)om.fi