Privacy policy: Whistleblowing channel

TIETOSUOJASELOSTE

Contents:

Document management:

Authors:	Privaon
Version:	1.0
Date:	22 June 2021
Approved by:	Taija Kautto / Lotta Väisänen
Owner:	Leena Laitinen
Review interval:	12 months

Version management:

Version	Date	Main content	Authors	Approved by
1.0	22 June 2021	First version	Privaon	Taija

1. Introduction

Updated 22 June 2021

Alko Oy (Alko) is committed to protecting your privacy and processing your personal data transparently and in accordance with current legislation and best practices. This privacy policy concerns the processing of personal data by Alko in connection with the maintenance of its whistleblowing channel. This privacy policy applies to personal data concerning those using the whistleblowing channel: whistleblowers submitting reports and the persons that are the subject of a report. This privacy policy details exactly how Alko is committed to collecting, processing and protecting your personal data during and after the whistleblowing process.

Below you will find more detailed definitions of the concepts we have used in this privacy policy.

"Personal data"	Personal data means all the identified and identifiable data relating to a person. For example, name, social security number, location data, network identification information, and address details.
"Sensitive data"	"Sensitive personal data" refers to personal data that reveal personal characteristics such as race or ethnic origin, political opinions, religious or philosophical beliefs, union membership, genetic or biometric data, or information about a person's health, sexual behaviour or sexual orientation.
"Processing personal data"	Processing personal data means all of the information processing operations that are targeted at personal data, either automatic or manual. Examples of processing personal data include collecting, saving, storing, editing, altering, removing or deleting data.
"Data subject"	The identified or identifiable natural person whose data is being processed. For instance, a job applicant or customer.
"Controller"	A natural person, legal person, authority, agency or other body that, either together or with another party, defines the purposes and methods for processing personal data.
"Joint controller"	If at least two controllers jointly define the purposes and methods for processing personal data (why and how personal data are processed), they are joint controllers. Joint controllers mutually and transparently define each area of responsibility in order to comply with the obligations laid down in legislation.

1. The use and processing of personal data

We collect and process personal data only to the extent that is required to perform Alko's whistleblowing process. The legal basis for processing your personal data is Alko's legal obligation* to maintain a whistleblowing channel. In addition, this channel can be used for the processing of other reports that come to light through it.

Personal data is primarily collected from the report submitted by the whistleblower and the investigation carried out on the basis of the report.

The reason why we are processing personal data will define what information we collect at any given time and for what purpose. We will only process the following personal details about you on the legal grounds specified below:

- **Data collected on the whistleblower:** As a rule, the whistleblowing channel is anonymous and Alko will not collect your personal data. Alko only collects personal data that the whistleblower voluntarily divulges in the report. Generally collected data is limited to name and contact information, if the whistleblower wishes to disclose them.
- **Information to be collected about the person who is the subject of the report:** The content of the report is case-specific and depends on what the whistleblower has stated. The nature of the report largely determines what kinds of personal data Alko will need to process the case. For instance, personal data concerning criminal convictions and misdemeanours is essential for investigating misconduct. The whistleblower may have included details that are unnecessary for the investigation of the case or other such miscellaneous information that does not have to be collected. Part of this information may involve specific categories of personal data or be otherwise sensitive. Alko assesses whether the information is necessary during the investigation of the case.

Alko does not process personal data on whistleblowers or the persons who are the subjects of such reports for other purposes.

* The legal obligation may be based on the laws of the European Union or its member states. In order to comply with the legal obligations of a controller, the controller may have to process personal data. The legal obligation may apply to controllers in both the private and public sectors. General examples of legal obligations are the duty of an employer to report information on the pay of employees to the tax authorities and the obligation of financial institutions to report suspicious business transactions to the authorities.

2. Sensitive data

Certain categories of personal data are classified as "sensitive personal data". Sensitive personal data will reveal personal characteristics such as race or ethnic origin, political opinions, religious or philosophical beliefs, union membership, genetic or biometric data, or information about a natural person's health, sexual behaviour or sexual orientation.

The processing of sensitive data is only permitted if said processing is necessary to comply with our legal obligations or with your express consent.

Alko processes sensitive personal data only to the extent necessary to investigate a whistleblowing report and when said processing is essential to comply with the obligations and special rights of Alko or the data subject with respect to labour rights, social security and social protection, or when said processing is vital for setting, implementing or safeguarding legal requirements.

3. Data disclosure and transfer

Alko is committed to processing your personal data confidentially. The collected personal data are only disclosed to parties outside Alko Oy on the basis of either regulations that permit such disclosure or Alko's legitimate interests (such as the right to protect property). Your personal data will only be disclosed to third parties for the following purposes:

- To the authorities, such as the Police, when official measures, such as a criminal investigation, are required to investigate the matter.

When processing collected data, we also use subcontractors and service providers (such as for technical maintenance) that have the right to process your data only to the extent required to provide the agreed services. This means that they cannot use your data for their own purposes. Our contractual terms and conditions require our partners to comply with data processing legislation and ensure adequate data security.

Your personal data will not be transferred outside the European Union or the European Economic Area.

4. Data security

Alko has implemented appropriate technical and organisational data security mechanisms to prevent the deletion and misuse of your personal data, as well as any other similar unlawful access to data. These mechanisms include firewalls, encryption and machine room security.

Alko uses access control and the granting of user rights and their supervision to restrict internal access to your personal data within the organisation. Your personal data will only be processed by employees that have the right and need to do so in order to carry out their job.

5. Access to information and exercising your rights

As a rule, you have the right to check what data we have collected about you and to say how we may use that data. Due to the nature of the processing of data in the whistleblowing channel, not all requests can necessarily be implemented on the basis of the obligations set forth in whistleblowing legislation if the implementation of the request would jeopardise the processing of reports.

In this section, we will detail your rights under current legislation and how to exercise them:

- **Right to check and correct data**

You have the right to check what data we have collected about you, or to receive assurance that no data about you is being held in our filing system. If there are any errors, inaccuracies or other deficiencies in your data, you can request us to correct or add information. Due to the nature of data processing in the whistleblowing channel, it is essential to evaluate the rights and interests of all parties in connection with the implementation of a request to check data. The right of a data subject to check data may be restricted in certain cases if it would have an adverse impact on the rights or freedoms of other parties.

- **Restricting or objecting to data processing**
  If your data is incorrect in some respect (for example, it is outdated), you have the right to request a temporary restriction on the processing of your data until we have verified its accuracy. Whenever the processing of your personal data is based on the controller's legitimate interest, you have the right to object to the processing of your personal data. We will then no longer be able to process your personal data, unless we can present a justifiable reason why this processing is so important and why it can be considered weighty enough to supersede your rights. We will also be allowed to continue processing your data if we need it to prepare, present or defend a legal claim.

- **Right to have data removed (Right to be forgotten)**
  In certain circumstances, you have the right to be forgotten. In that case, we will remove all the data we have collected about you, unless this data is still required for the purposes it was originally collected for (such as to investigate a misdemeanour). Unless there are other justifiable grounds for processing your data, we will also remove your data if you object to the processing of your personal data, or if the processing of your personal data is based on your personal consent and you withdraw this consent. However, please note that we may have statutory legal obligations to retain your personal data for a certain period of time.

- **Right to appeal**
  In addition to the aforementioned rights, you also have the right to appeal to the supervisory authorities with regard to the processing of your personal data.

How can I submit a request to check personal data?
You can request to check your personal data and exercise your data protection rights by emailing tietosuoja@alko.fi.

6. Data retention

As a rule, we retain whistleblowing report data while the case is being investigated. When a case has been processed and closed, the reported data will be deleted from the whistleblowing system or the report will be archived anonymously such that identifiable data is irrevocably removed from the report and an individual person can no longer be identified from the information in the report.

7. Amendments to this privacy policy

We will regularly update this privacy policy, both as we develop our data protection practices and as a consequence of legislative amendments. We recommend that you check for changes in our privacy policy from time to time.

A summary of the latest changes to our privacy policy has been placed at the beginning of this document, to make it as easy as possible for you to monitor the processing of your personal data.

8. Controller and contact details

Controller	**Contact person in matters related to the register**
Alko Inc Arkadiankatu 2 P.O. Box 99, 00101 HELSINKI Tel. +358 20 711 11 Fax +358 20 711 5386 Business ID: 1505551-4 Domicile: Helsinki	Alko Customer Service Arkadiankatu 2 P.O. Box 99, 00101 HELSINKI tietosuoja@alko.fi +358 (0)20 692 771 (local network rate)