# Privacy policy: Closed-circuit television, security occurrence and visitor management register

**PRIVACY POLICY**

**Contents:**

## Introduction

Updated 5 November 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 covers the processing of personal data that Alko carries out in order to organise closed-circuit television surveillance, handle security occurrences and manage visitors. This privacy policy applies to everyone who moves about in and around Alko premises.
This privacy policy details exactly how Alko is committed to collecting, processing and protecting your personal data.

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. |
| "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 example, a customer or employee. |
| "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. |

## 1. The use and processing of personal data

The legal basis for processing personal data in this register is Alko's legitimate interest*. We collect and process personal data only to the extent that is required for the following purposes:

The purpose of the **closed-circuit television (CCTV) system** is to protect property on the premises, prevent crime, and assist in solving crimes and misdemeanours. Using CCTV helps us to ensure public safety and safeguard the legal protection of both our customers and employees. The CCTV system is also used to protect the safety and security of employees. For this purpose, the register collects the personal data of individuals on the premises or in their immediate vicinity. In addition, we may store and use the material we collect to make, present and defend a legal claim. The register also stores data arising from a customer or employee relationship, membership or comparable relationship.

The purpose of the **security occurrence system** is to collect data on security occurrences, crimes and disturbances on the premises. The data is used to form a situational picture of security on the premises to serve as the basis for carrying out security measures. The aim of this is to improve the occupational safety of employees on the premises. For this purpose, the register collects the personal data of individuals who commit crimes or cause disturbances and other security occurrences, either on the premises or in their immediate vicinity. Data entered into this system is also used to report offences to the police. Security status monitoring and the reporting of offences have been outsourced to Securitas Oy.

The purpose of the **visitor management system** is to manage visitor data and ensure the security of Alko's premises by permitting access only to authorised visitors. Personal data is processed for the purposes of organising meetings, inviting visitors to Alko's premises, granting access rights and monitoring visitors on the premises.

* "Legitimate interest" refers to data processing that forms an essential aspect of the controller's business and that the data subject can reasonably assume to be part of the controller's operations. The controller often has to process personal data in order to carry out business-related tasks. In this context, the processing of personal data cannot necessarily be justified on the basis of a statutory obligation or contractual grounds. However, the processing of personal data can be justified on the basis of 'legitimate interest'. Before personal data is processed on the basis of legitimate interest, the controller must always ensure that conducting business in accordance with this legitimate interest will not seriously violate the data subject's rights and freedoms.

Personal data is collected in the following manner:

- Data in the CCTV system consists of video footage that is recorded by the system's surveillance cameras of people moving about in the surveillance area. To inform people that they are under video surveillance, premises with CCTV are equipped with signs and/or labels that state "This store is protected by video surveillance."
- The personal data of individuals suspected of committing crimes or causing disturbances or other security occurrences is recorded in the system by Alko employees.
- Data in the visitor management system is recorded by the event host or a person authorised by them, or by visitors themselves.

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 data about you on the legal grounds specified below:

- **CCTV register:** camera footage, date and time
- **Security occurrence register:** name, personal identification number, contact details and identifying image from the CCTV system
- **Visitor management system:** Name, email, phone number, company, title, name of host

## 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.

Alko does not process sensitive personal data for the purposes of carrying out CCTV surveillance or managing security occurrences and visitors.

## 3. Data disclosure and transfer

Alko is committed to protecting the confidentiality of your personal data, and we will disclose your data to specific partners when necessary only in the following instances:

- In suspected criminal offences, data may be disclosed to the police, other equivalent authorities and between locations within the company to a limited extent.

When processing the personal data we collect, we also use the security monitoring centre and lobby services provided by our partners. These partners have the right to process your personal data only to the extent that is necessary in order to provide the services in question. 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 disclosed to any parties outside the European Union and 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.

The processing of your personal data is also restricted by access control and the management of user rights. 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

You have the right to check what data we have collected about you and to say how we may use that data. You can decide whether you wish to receive email communications from us. In certain circumstances, you have the right to have your data removed or request your data to be transferred to another controller. In this section, we will detail your rights under current legislation and how to exercise them:

- **Right to withdraw consent**
  When your personal data is being processed on the basis of personal consent from you, you have the right to withdraw this consent at any time. For example, you may at any time end your subscription to our newsletter by withdrawing your consent.

- **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.

- **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 transfer data from one system to another**
  You may request your personal data to be transferred, in which case we will send your personal data to you in machine-readable format, so you can either retain it yourself or transfer it to another controller. If it is technically possible, we will also transfer your data directly to another controller at your request. This is only possible in situations in which we are processing your personal data on the basis of your personal consent or contractual grounds, and only covers data that you have provided us with yourself.

- **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 submit a request to check your personal data at an Alko store or by emailing us at tietosuoja@alko.fi.

Before disclosing personal details, we will need to verify your identity, so that we do not disclose your data to the wrong person. You can prove your identity either at an Alko store when submitting your request, or by logging into the online shop with your access codes.

## 6. Data retention

We will only retain your data for as long as required in order to carry out the purposes specified in Section 1, and always within the current boundaries of the law.

After this, your data will either be deleted or made unidentifiable, by irreversibly converting it into a format in which individual persons can no longer be identified.

The retention period is determined by the duration of your customer relationship or whether any action relating to misdemeanours is still pending. A customer's personal data will be stored until the customer requests its removal from the register, unless legislation prevents the removal of such data.

- **CCTV register:** unless a recording is required for an ongoing investigation, the system will automatically record new footage over existing footage a maximum of ten weeks after the original footage was recorded. If a recording is required for an investigation, it will be deleted after the case has been concluded and any statute of limitations period ends.
- **Security occurrence register:** In the case of CCTV recordings, data will be deleted two years after the occurrence.
- **Visitor management system:** 100 days from your last visit.

You can also request corrections to your data by contacting tietosuoja@alko.fi.

## 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<br>Arkadiankatu 2<br>P.O. Box 99, 00101 HELSINKI<br>Tel. +358 20 711 11<br>Fax +358 20 711 5386<br>Business ID: 1505551-4<br>Domicile: Helsinki | Alko Customer Service<br>Arkadiankatu 2<br>P.O. Box 99, 00101 HELSINKI<br>tietosuoja@alko.fi<br>+358 (0)20 692 771 (local network rate) |