



Whistleblowing system – Data protection information

We take data protection and confidentiality very seriously and adhere to the provisions of the EU General Data Protection Regulation (GDPR) as well as current national data protection regulations.

Please read this privacy information carefully before submitting a report.

Controller and data protection contact:

The controller for the data processing is:

ALDI Technology Support Sp. z o.o.
ul. Fabryczna 1
31-553 Kraków

The data protection department can be reached by email at dataprotection@aldi-techhub.pl and by post at the above-mentioned address.

Purpose of the whistleblowing system, legal basis and provider

The whistleblowing system (BKMS® System) serves for securely and confidentially receiving, processing and managing reports concerning violations of the compliance rules. ALDI has a legal obligation to provide a whistleblowing system.

The whistleblowing system is technically provided by EQS Group AG, Bayreuther Str. 35, 10789 Berlin. EQS Group AG is a company specialised in whistleblowing systems, which has been commissioned by ALDI Einkauf SE & Co. oHG as a subprocessor. The legal foundation for this processing of personal data is Article 6(1)(c) GDPR in conjunction with the provisions of the Act of 14 June 2024 on the protection of whistleblowers, and Article 6(1)(f) GDPR. Our legitimate interest is discovering and preventing abuse and thereby averting damage to the company, its employees and customers.

Processing of personal data

Personal data and information entered into the whistleblowing system are stored in a database of a high security data centre operated by EQS Group AG. Only the competent and authorised employees of the ALDI Nord Group have access to the data. EQS Group AG and other third parties do not have access to the data. This is ensured in the certified procedure through extensive technical and organisational measures.

All data are stored encrypted with multiple levels of password protection so that access is restricted to a very small selection of expressly competent and authorised persons.



Type of personal data collected

Use of the whistleblowing system takes place on a voluntary basis. If you submit a report via the whistleblowing system, we collect the following personal data and information insofar as it is shared by you:

- your name,
- where you are employed, and
- the names and other personal data of persons whom you list in your report, if applicable.

Confidential handling of reports

Incoming reports are received by a small selection of expressly competent and authorized specially trained employees of the responsible Compliance department and are always handled confidentially. The employees of the Compliance department evaluate the matter and perform any further investigation required by the specific case.

During the processing of a report or the conducting of a special investigation, it may become necessary to forward reports to other parties. We will always ensure that the applicable data protection regulations are complied with when sharing reports.

All persons who receive access to the data are obligated to maintain confidentiality.

Information about the accused

We are legally obligated to inform accused parties of any reports received against them as soon as the disclosure of this information no longer jeopardises the investigation. Your identity as a whistleblower, if you even reveal it, will generally not be disclosed.

Your rights

Pursuant to European data protection legislation, you and the persons named in the report have a right of access, rectification, erasure, restriction of processing and right to object to the processing of your personal data. If the right to object to the processing of the personal data is invoked, the necessity of the stored data for the examination of a report will be evaluated immediately. Data that are no longer needed will be deleted at once. You also have the right to appeal with the supervisory authority.



Retention period of personal data

Personal data is retained for as long as necessary to clarify the situation and perform a final assessment or for as long as a legitimate interest exists on the part of the company or retention is required by law. After the report processing is concluded, the data will be anonymised and deleted in accordance with statutory requirements.

Use of the whistleblowing portal

Communication between your computer and the whistleblowing system takes place over an encrypted connection (SSL). Your IP address will not be stored during your use of the whistleblowing system. In order to maintain the connection between your computer and the BKMS® System, a cookie is stored on your computer that merely contains the session ID (a so-called session cookie). This cookie is only valid until the end of your session and expires when you close your browser.

It is possible to set up a postbox within the whistleblowing system that is secured with an individually chosen pseudonym/user name and password. This allows you to send reports either by name or in an anonymous, safe way. This system only stores data inside the whistleblowing system, which makes it particularly secure. It is not a form of regular e-mail communication.

Note on sending attachments

When submitting a report or an addition, you can simultaneously send attachments. If you wish to submit an anonymous report, please take note of the following security advice: files can contain hidden personal data that could endanger your anonymity. Remove this data before sending. If you are unable to remove this data or are uncertain about how to do so, copy the text of your attachment into your report text or send the printed document anonymously to the address listed in the footer, citing the reference number received at the end of the reporting process.