Privacy policy
Information on data protection in the context of the whistleblower system

Below you will find information about the collection, processing and use of personal data within the scope of the whistleblower system when you submit a suspicious activity report by e-mail, telephone call, letter or personal appearance at the Audi Investigation Office. Please read this Privacy Policy carefully before submitting a suspicious activity report.

Type of personal data collected

The use of the whistleblower system is voluntary. We collect the following personal data and information when you submit a suspicious activity report via the whistleblower system:

- Your name, if you reveal your identity
- Your contact details, if you provide them
- Whether you are employee of AUDI AG or not
- The fact that you have made a suspicious activity report via the whistleblower system
- Where applicable, the names of persons and other personal data of the persons named in your suspicious activity report

Notes on sending attachments

When submitting a suspicious activity report or supplementary information, you have the option of sending attachments to the responsible employees of AUDI AG. If you wish to submit a suspicious activity report anonymously, please note the following security instructions: Files may contain hidden personal data that may compromise your anonymity. Remove this data before submitting. If you are unable to remove this data or if you are not sure how to do so, copy the text of the attachment into an e-mail and send it to whistleblower-office@audi.de stating the reference number that you can find in the acknowledgement of receipt or send the printed document anonymously, stating the file number that you can find in the acknowledgement of receipt, to AUDI AG, whistleblower system, 85045 Ingolstadt.

Purpose of the whistleblowing system and data processing / legal basis

The whistleblower system is used to securely and confidentially receive and process information about (suspected) violations of laws or internal regulations to the detriment of AUDI AG or the Volkswagen Group.

The processing of personal data within the scope of the whistleblower system is based on the legitimate interest of AUDI AG in the detection and prevention of grievances and the associated avoidance of damage and liability risks for AUDI AG or the Volkswagen Group (Art. 6 (1) (f) GDPR in conjunction with §§ 30, 130 OWiG). Section 4.1.3 of the German Corporate Governance Code also provides for the establishment of a whistleblower system to give employees and third parties a suitable opportunity to provide protected suspicious activity reports of legal violations within the company. Until now, the processing of personal data within the whistleblowing system has also been necessary to fulfil a legal obligation (Art. 6 (1) (c) GDPR).

With regard to a suspicious activity report by an employee of AUDI AG, the processing also serves to prevent criminal offences or other legal violations in connection with the employment relationship (§ 26 (1) BDSG).

The processing of transmitted personal data within the whistleblowing system may also be based on consent (Art. 6 (1) (a) GDPR).

As a whistleblower, you are able to use the whistleblowing system anonymously, i.e. without providing any information about your identity, without giving reasons. If you decide to intentionally and consciously disclose your identity to AUDI AG, AUDI AG requires your consent. AUDI AG will treat your identity confidentially during the internal and extrajudicial or extra-official steps of any investigation. However, it may be necessary to disclose your identity when communicating with authorities and/or courts. In certain cases, AUDI AG is also obliged under data protection law to inform the accused person of the allegations made against him within one month at the latest.

Your identity as a whistleblower will not be disclosed – insofar as this is permissible in accordance with Art. 14 para. 3 lit. a GDPR.

Please note that AUDI AG does not require your consent if it concerns personal data provided in the description of the facts, in particular when describing your participation in or being affected by the events described. In this respect, the processing is based on a legitimate interest of AUDI AG to investigate, remedy and sanction criminal offences and serious regulatory violations committed by Group employees.

You have the right to revoke your consent to the processing of your name in your capacity as a whistleblower with effect for the future at any time and without giving reasons. Please send your revocation to the following address:

AUDI AG
Hinweisgebersystem
85045 Ingolstadt, Germany
E-Mail: whistleblower-office@audi.de

As a rule, however, consent can only be revoked within one month of receipt of the suspicious activity report, as in certain cases AUDI AG is obliged under Art. 14 para. 3 lit. a GDPR to inform the accused person of the allegations made against him and the investigations carried out against him within one month, including the storage, the type of data, the purpose of the processing and the identity of the controller and, if applicable, the whistleblower and a cessation of data processing of the identification data of the reporter is then no longer possible. In addition, the processing of the data has already progressed so far after that time that deletion is no longer possible. However, the revocation period can also be shortened, sometimes considerably. This is the case if the nature of the suspicious activity report requires the direct involvement of an authority or a court. Once we have disclosed the name to the authority or court, it will be in our case files as well as with the authority or court and can no longer be deleted.

In the event of revocation, AUDI AG will immediately delete your data specified in the declaration of consent (your name, your contact details and the fact that you made the suspicious activity report via the whistleblower system). The content of the suspicious

activity report made via the whistleblower system will continue to be used without you being named as a whistleblower. If the examination of your suspicious activity report reveals that it was intentionally made incorrectly, Audi may be legally obliged to archive it or require further processing to assert, exercise or defend legal claims.

Responsible body and data security

1. Responsible body for suspicious activity reports concerning AUDI AG

The body responsible for data protection of the whistleblowing system is AUDI AG, Auto-Union-Straße 1, 85057 Ingolstadt, provided that the suspicious activity report concerns AUDI AG.

All data is stored in encrypted form, so that access is restricted to a very narrow circle of expressly authorized persons of AUDI AG.

AUDI AG has appointed a data protection officer. Data subjects can contact the data protection officer of AUDI AG directly:

AUDI AG
Data protection officer
85045 Ingolstadt, Germany
E-Mail: datenschutz@audi.de

2. Responsible bodies for suspicious activity reports concerning a Group company outside AUDI AG

The entities responsible for processing your personal data are AUDI AG and the affiliated companies and subsidiaries ("Volkswagen Group") that are directly and indirectly majority-owned or majority-controlled with the Volkswagen Group, insofar as the suspicious activity report relates to a Group company outside AUDI AG. The Volkswagen Group has defined the basis for the joint processing of your personal data and coordinated the responsibilities within the Volkswagen Group in a Group-wide agreement on the treatment of personal data for compliance purposes. The following information also summarizes the substance of this Agreement for you. Further information can be found at the end of the data protection notice under "Joint responsibility of the Volkswagen Group". In addition, you can obtain further information at any time and free of charge at the address AUDI AG, whistleblower system, 85045 Ingolstadt or at the e-mail address whistleblower-office@audi.de.

All data is stored encrypted, so access is restricted to an extremely small circle of expressly authorized persons.

AUDI AG has appointed a data protection officer. Affected parties can contact the data protection officer of AUDI AG directly:

AUDI AG
Data Protection Officer
85045 Ingolstadt, Germany
E-Mail: datenschutz@audi.de

Confidential treatment of suspicious activity reports

Incoming information is processed by a small group of expressly authorized and specially trained employees of the Compliance department of AUDI AG and treated confidentially in any case. The employees of AUDI AG review the facts and can carry out further case-related investigations.

In accordance with the Data Protection Act, AUDI AG is obliged in certain cases to inform the suspicious person of the allegations made against it. This is a legal obligation in cases where it can be objectively demonstrated that the disclosure of information to the suspicious person can no longer have an adverse effect on the special audit concerned. To the extent legally possible, your identity as a whistleblower will not be disclosed to the extent permitted by Art. 14 (3) (a) GDPR and steps will also be taken to ensure that no conclusions can be drawn about your identity as a whistleblower.

Confidentiality cannot be guaranteed if you intentionally provide incorrect information with the aim of discrediting a person (denunciation).

During the processing of a suspicious activity report or the conduct of a special investigation, it may be necessary to forward suspicious activity reports to other employees of AUDI AG or its subsidiaries and their employees or Volkswagen AG and its subsidiaries. This is the case, for example, if the suspicious activity reports relate to activities in subsidiaries of the Volkswagen Group. To the extent necessary for clarification, data may be transferred to subsidiaries of the Volkswagen Group in a country outside the European Union or the European Economic Area on the basis of appropriate data protection guarantees for the protection of data subjects. Please note that not all third countries have an adequate level of data protection recognized by the European Commission. AUDI AG will only transfer your personal data to third countries to the extent permitted by Articles 44 – 49 GDPR. Insofar as AUDI AG relies on appropriate guarantees pursuant to Article 46 (2) GDPR for the transfer to third countries (e.g. standard contractual clauses or binding corporate rules), AUDI AG will take additional technical and/or organizational measures to the extent necessary to maintain adequate protection of your personal data. Data subjects have the right to obtain from AUDI AG a copy of the appropriate or appropriate guarantees for the transfer of personal data to third countries.
When passing on suspicious activity reports, we always ensure compliance with the applicable data protection regulations.

Other possible categories of recipients are law enforcement authorities, antitrust authorities, other administrative authorities, courts as well as international law firms and auditing firms commissioned by AUDI AG or the Volkswagen Group, insofar as this is required by law or data protection law.

All persons who gain access to the data are obliged to maintain confidentiality.

Duration of storage of personal data

Personal data will be kept for as long as necessary for clarification and final assessment, if the company has a legitimate interest or if storage is required by law. This data will then be deleted in accordance with the statutory provisions.

Rights of the data subject

In accordance with European data protection regulations, you and the persons named in the suspicious activity report have a right of access, correction, deletion and restriction of the processing of your personal data as well as a right to object to the processing of your personal data and, in certain cases, the right to data portability.

Your right to object

You have the right to object to the processing of your personal data for reasons arising from your particular situation. The prerequisite for this is that the data processing is carried out in the public interest or on the basis of a balance of interests. The objection can be made form-free and should be made to the contact details listed in this data protection notice. If the right of objection is exercised, we will immediately check to what extent the stored data is still necessary, in particular for the processing of a suspicious activity report. Data that is no longer required will be deleted immediately.

Your right of withdrawal

You can also revoke your consent at any time. In this context, please note the information under "Purpose of the whistleblower system and data processing / legal basis".

Further information and the possibility to assert your rights can be found at:

Data Subject Rights
AUDI AG, GDPR Rights of Data Subjects, 85045 Ingolstadt

If you have general questions about this data protection notice or the processing of your personal data by Audi AG, please use the following contact options:

AUDI AG
Hinweisgebersystem
85045 Ingolstadt, Germany
E-Mail: whistleblower-office@audi.de

You also have the right to lodge a complaint with the competent data protection authority. This is for example:

> Bayerisches Landesamt für Datenschutzaufsicht
> Promenade 18
> 91522 Ansbach, Germany
> Germany
> https://www.lda.bayern.de

Further information on data protection at AUDI AG can be found here:
https://www.audi.com/en/privacy-policy/

In order to safeguard your rights in the event of a suspicious activity report concerning a Group company outside AUDI AG, please contact the Volkswagen Group company to which you submitted your report. The companies of the Volkswagen Group support each other in answering your request.

Joint responsibility of the Volkswagen Group

In a Group-wide agreement, the Volkswagen Group regulates the scope of roles and responsibilities as well as mutual obligations with regard to the responsibility for the joint processing of personal data in the sense of a whistleblower system (see above "Purpose of the whistleblower system"). Joint responsibility pursuant to Article 26 GDPR exists when several parties jointly determine the purposes and means of processing personal data. Such joint responsibility is effectively limited to the Volkswagen Group companies associated with you, as other companies may have only read access to data or no access at all in the shared processes and systems.

The data is processed within the European Union and in countries outside the European Union. In their agreement, the parties have ensured by appropriate regulations that processing outside the European Union follows the same strict rules and requirements as processing within the European Union.

In the agreement, all parties have committed themselves to comply with the data protection laws applicable to them, in particular the strict requirements of the GDPR, such as the principle of data minimization, and to carefully implement these obligations. The respective task and the system operators shall ensure that the processing of the data within the systems takes place within a framework corresponding to the requirements of the applicable data protection law. In addition, the necessary data protection impact assessments were carried out for all tasks of the compliance function for which joint responsibility is to exist. A data protection impact assessment is an assessment of the impact of the intended processing operations on the protection of your personal data.

AUDI AG, which imports data into the joint process, or another data-modifying company will ensure that this is done in accordance with applicable data protection laws, which is ensured by appropriate measures such as obtaining consent. The companies also ensure compliance with the confidentiality and integrity of the data, in particular through a confidentiality obligation of persons who have access to the data of the process or an IT system. Data secrecy is ensured by technical and organizational measures for which each Volkswagen Group company is responsible within the scope of its IT systems. In addition, all companies are obliged to implement, regularly review and, if necessary, update these data protection measures in relation to joint responsibility for personal data.

In the event of a possible personal data breach, companies shall immediately inform each other and remedy the situation through a coordinated reporting procedure. Where appropriate, the Companies shall notify the competent supervisory authority and/or inform the persons affected by the data breach.