

Privacy Statement

Entity responsible for processing your personal data

Telekom Austria AG (“**A1**”), as a controller, collects and processes your data in the BKMS whistleblowing system (“**BKMS Whistleblowing System**”). If an alleged violation involves other A1 Group companies, the following A1 Group companies might be data controllers to the extent it is necessary to address the violation: A1 Telekom Austria AG, Unitary enterprise A1 (Belarus), A1 Bulgaria EAD, A1 Hrvatska d.o.o., A1 Digital International GmbH, A1 Digital Deutschland GmbH, A1 Makedonija DOOEL, paybox Bank AG, A1 Slovenija d.d. and A1 Srbija d.o.o.

The BKMS Whistleblowing system is operated on behalf of A1 by EQS Group AG. It offers a secure, confidential way to receive and process reports about serious violations of the law and other misconduct within A1 Group.

You can contact Telekom Austria AG or our data protection officer at the following address:

Lassallestraße 9, 1020 Vienna

Categories of collected personal data

If you choose to share this information, A1 may collect and process various categories of your personal data required for operation of the BKMS Whistleblowing System, including:

- First and last name;
- Contact information (e.g., email address, phone number);
- Position and professional affiliation; and
- Information about the circumstances of your complaint (documents, emails, images and other content).

Purpose of processing personal data

A1 processes your personal data solely to provide you with whistleblowing reporting channels and to investigate any improper conduct within A1 or by business partners in connection with A1.

We rely on the following legal bases when collecting and processing your personal data:

- **Legal obligation** under Article 6(1)(c) of the EU General Data Protection Regulation (“EU GDPR”). We process your personal data to comply with the legal obligations in relation to whistleblowing.
- **Legitimate interest** under Article 6(1)(f) of the EU GDPR. In particular, we process your personal data to protect our overriding legitimate interest in detecting and preventing crimes and other misconduct within A1 Group and protecting A1 Group and its employees from the potentially detrimental effects of such crimes and misconduct.

Confidential handling of personal data

We encourage you to disclose your identity when you submit a suspected violation. Many investigations can be conducted more effectively if the name of the whistleblower is known, as the investigating officer is able to ask you additional questions and provide their feedback.

However, A1 protects the anonymity of reporters who do not want to reveal their identity. If you would like to remain anonymous, do not submit any personal information, e.g. your name or relationship to the offender. In case you upload documents, please also make sure to remove all signs, that could be used to discover your identity.

Please be assured that only a small number of authorised and trained A1 employees will handle whistleblowing reports incoming through the BKMS Whistleblowing System. All persons who receive access to the data are obligated to maintain confidentiality.

Access of third parties to personal data

Apart from a small number of A1 employees, no other parties, including EQS Group AG, have access to personal data in non-encrypted format.

During the processing of a report or the conduction of an investigation, it may become necessary to share reports with additional employees of A1 Group, e.g. if the report refers to incidents in A1 subsidiaries. The latter may be based in countries outside the European Union or the European Economic Area with different regulations concerning the protection of personal data. We always ensure that the applicable data protection regulations are complied with when sharing reports.

If the actions or occurrences you reported are prosecuted under criminal law, it is possible that we will be required by law to share your data with the officials investigating the situation. We may also be required by law to provide certain government agencies, including, without limitation, government investigation agencies or courts with information about reported compliance violations.

Protection of personal data

Your personal data entered into the BKMS Whistleblowing System is stored in an encrypted, password-protected form in a database which is operated by EQS Group AG on A1's behalf. The data is stored at a data center on a high-security level in Germany.

A1 has also implemented technical and organizational security measures (e.g., access controls, encryption, physical security and restricted access etc.) to protect your personal data collected via BKMS Whistleblowing platform and any subsequent compliance investigations against unauthorized access, loss or destruction.

Retention period

We only store your data for as long as is necessary to fulfill the purpose for which the data was collected or as long we need it to comply with legal requirements. Once the report processing has been completed, this data will be deleted in accordance with the statutory requirements.

Rights in respect to personal data

Right of Access: You can ask us to confirm whether and to what extent we process your personal data. Simply use our contact details indicated in this Privacy Statement.

Right to Rectification: If we process your personal data that is incomplete or incorrect, you may request that we correct or complete it at any time.

Right to Erasure: You can request us to delete your personal data if we process it unlawfully or if the processing disproportionately interferes with your legitimate protection interests. Please note that there may be reasons that prevent an immediate deletion, e.g. in the case of legally regulated storage obligations.

Right to Restriction of Processing: You can ask us to restrict the processing of your data if:

- you dispute the accuracy of the data for a period that allows us to verify the accuracy of the data,
- the processing of the data is unlawful, but you refuse to delete it and instead demand a restriction on the use of the data,
- we no longer need the data for the intended purpose, but you still need this data to assert or defend legal claims, or
- you have objected to the processing of the data.

Right to Object: If we process your data for the performance of tasks in the public interest, for the exercise of official authority or if we refer to the necessity of safeguarding our legitimate interest

during processing, you may object to this data processing if there is a predominant interest in protecting your data.

Right to Appeal: If you are of the opinion that we violate Austrian or European data protection law when processing your data, please contact us to clarify any questions you may have. Of course, you also have the right to complain to the Austrian Data Protection Authority (www.dsb.gv.at) as well as to a supervisory authority within the EU.

This privacy notice was last updated in August 2024.