



TELEKOM AUSTRIA AG

DATA PRIVACY STATEMENT FOR SUPPLIERS

1. GENERAL INFORMATION ABOUT THIS DATA PRIVACY STATEMENT

This Privacy Statement is addressed to:

- our current or prospective suppliers, service providers and other externals who are individuals; and
- employees, representatives and/or contact persons of our current or prospective suppliers and service providers.

Telekom Austria AG processes information about you which constitutes "personal data" and decides why and how it is processed, thereby acting as the "controller". We take the protection of your personal data very seriously and comply with European and national data protection regulations, in particular the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR) and the Austrian Data Protection Act (DSG).

The following Privacy Statement explains which personal data we process about you, to what extent and for what purpose.

2. WHO IS RESPONSIBLE FOR THE DATA PROCESSING?

The following entity is responsible for the data processing:

Telekom Austria AG
Lassallestraße 9
1020 Vienna

Should you have any question in relation to the processing of your personal data, please contact us at dataprotection@a1.group.

3. WHICH PERSONAL DATA IS PROCESSED?

We may process your personal data which is either directly provided by you or by our supplier or service provider (i.e. your employer).

Such personal data may include:

- General personal information (e.g. name, date of birth, postal address, e-mail address, telephone number);
- Business contact data (e.g. name of the employer, postal address, e-mail address, telephone number) and related information (e.g. function, department);
- Personal data required for the evaluation and selection of bidders according to the underlying tender conditions (e.g. personal data included in the tender documents, offers, bidder's self-disclosures including business contact data of the supplier's employees);
- Personal data relating to suspected and actual criminal conduct, criminal records or information about criminal proceedings for criminal or unlawful conduct provided to ensure compliance with our legal and regulatory obligations; and/or
- For any person who requires access to our premises and/or IT infrastructure to provide services, we may collect the identification and electronic identification data (e.g. access rights, login, passwords, badge number, IP address, online identifiers/cookies, logs, access and connection times, image recording or sound such as badge pictures, CCTV or voice recordings).

You are under no obligation to provide us with your personal data. However, if such personal data is necessary for us to manage our relationship with you or your employer (e.g., information necessary to evaluate your qualifications, meet our regulatory and legal obligations or ensure our security interests), and you fail to provide personal data when requested, we may not be able to retain your services.

4. FOR WHAT PURPOSE DO WE PROCESS THE PERSONAL DATA?

We always process the relevant personal data to achieve a specific purpose. For instance, we process your personal data to:

- (a) organise the tender process, conclude and perform existing contracts;
- (b) manage our suppliers and service providers throughout the procurement process and contract performance;
- (c) conduct vendor integrity checks on existing and potential contractual partners before concluding contracts and at regular intervals after concluding contracts in order to comply with our legal obligations (in particular with regard to combating money laundering and/or corruption);
- (d) ensure compliance and reporting (such as complying with our policies and local legal requirements, managing alleged cases of misconduct or fraud, conducting audits and defending litigation);
- (e) ensure the security and safety of our information, business premises and facilities, services, customers and employees;
- (f) grant you access to our premises and/or systems to allow you to perform services;
- (g) manage and protect our technology resources (e.g. cyber-risk management, infrastructure management and business continuity);
- (h) archiving and record-keeping;
- (i) billing and invoicing; and/or
- (j) keeping you informed of news, updates and other information related to our business and that of other companies in A1 Group.

5. WHICH LEGAL BASES ARE RELEVANT FOR THE PROCESSING OF PERSONAL DATA?

We will only process your personal data if we have a proper legal basis under the applicable data protection law. In particular, we will only process your personal data if:

1. The processing is necessary **to perform our contractual obligations** towards you or to take pre-contractual steps at your request (GDPR Article 6(1)(b)), for example, in cases specified in paragraphs 4(a), (b), (f) and (i) above;
2. We have obtained your **prior consent** (GDPR Article 6(1)(a)), for example, in cases specified in paragraphs 4(j) above;
3. The processing is necessary **to comply with our legal or regulatory obligations** (GDPR Article 6(1)(c)), for example, in cases specified in paragraphs 4(c), (d), (e), (h) and (i) above; and/or
4. The processing is necessary for **our legitimate interests** and does not unduly affect your interests or fundamental rights and freedoms (GDPR Article 6(1)(f)), for example, in cases specified in paragraphs 4(a), (b), (c), (d), (e), (f) and (g) above.

As A1 companies form part of the critical infrastructure in their respective jurisdictions, we rely on our legitimate interest to manage and monitor the external individuals who have access to our premises, IT infrastructure, and any A1 data. For this reason, we run an internal programme to

clearly identify all externals by collecting and storing their personal data (e.g. name, email, phone number, birth date). This data allows us to ensure that each external worker and/or service provider has access strictly limited to the agreed scope of services and that the access is effectively terminated when required.

We further carry out video surveillance of our premises and territory in order to protect the company's assets, confidential information and ensure the security of our employees and visitors.

6. WHO ARE THE RECIPIENTS OF THE PERSONAL DATA?

We will only transfer your personal data to third parties if we have a valid reason for such transfer and to the extent such transfer complies with applicable law.

To achieve the purposes mentioned above, your personal data can be accessed by or transferred to the following categories of recipients on a need-to-know basis:

- our affiliated companies within the A1 Group;
- our personnel (including personnel in other companies of the A1 Group);
- our contract processors who carry out certain tasks for us, e.g. for IT and cloud services or tools for administration; and/or
- our legal and other professional advisors.

Even if we engage an external data processor, we remain responsible for the protection of your personal data. The above third parties will be contractually obliged to protect the confidentiality and security of your personal data and process your personal data in compliance with applicable law and purposes outlined above.

Your personal data can also be accessed by or transferred to a regulatory, enforcement, public body or court, where we are required to provide such information by applicable law or regulation.

7. IS PERSONAL DATA TRANSFERRED TO A THIRD COUNTRY?

Some of the recipients of your personal data may be located outside of the EU/EEA and process your data there. We will only use processors outside the European Union if (i) a European Commission adequacy decision has been made for the third country in question or (ii) if we have agreed appropriate guarantees or binding internal data protection regulations with the processor to ensure that the European level of data protection and the European data security standards are maintained.

8. HOW DO WE PROTECT YOUR PERSONAL DATA?

Our goal is to protect the personal data in our possession against accidental or unlawful destruction or alteration, accidental loss, unauthorised disclosure or access and against other unlawful forms of processing. We take effective technical and organisational measures to protect your data, and our employees are also trained in the handling of personal data.

9. HOW LONG IS THE PERSONAL DATA STORED?

We will only retain your personal data for as long as necessary to fulfil the purpose for which it was collected unless overriding legal or regulatory obligations require a longer or shorter retention period.

There is a possibility that the data may be anonymised instead of deleted. In this case, all personal references will be irretrievably removed, thus eliminating the data protection obligations to delete.

10. WHICH RIGHTS YOU MAY EXERCISE WITH REGARD TO THE PROCESSING OF 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. Please be aware that we cannot reveal any details about our business and trade secrets within the scope of our duty to provide information. To protect your data, it is necessary for us to carry out an identity check.

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 Data Portability: You may request that we make available to you the data you have entrusted to us for storage in a structured, common and machine-readable format, provided that:

- we process this data based on your given and withdrawable consent or for the fulfilment of a contract between us, and
- such processing is carried out using automated procedures.

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. You can object to the sending of an offer or advertisement at any time without giving reasons.

Right to Complain: 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.

11. HOW CAN YOU ASSERT YOUR RIGHTS?

If you wish to assert any of the above rights, please contact us at the address indicated in this Privacy Statement above.

Confirmation of Identity: When processing your inquiry, we may request additional information to confirm your identity, e.g. a legible copy of a valid photo ID with signature. This is to protect your rights and privacy.

Excessive Claiming of Rights: Should you exercise any of the above rights manifestly unfounded or particularly frequently, we may charge a reasonable processing fee or refuse to handle your request

12. HOW WILL YOU BE INFORMED OF THE CHANGES TO OUR PRIVACY STATEMENT?

Any future changes or additions to the processing of your personal data as described in this Privacy Statement will be notified to you through our usual communication channels (e.g. by email or via our internet websites).

This Privacy Statement was last updated in February 2025.