A1 Group Personal Data Privacy and Protection Policy

A1 Group Data Privacy Program

Version	**1.0**
Classification	Public
Document ID	PRI-POL-GRP-ENG-V**1.0**
Document status	APPROVED
Document owner	A1 Group Legal and General Counsel
Master copy location	A1 Group Privacy Portal
Last review date	02.03.2026
Effective date	02.03.2026

***Note**: This document is maintained in electronic form. Printed copies may differ from the current version.*

TABLE OF CONTENTS

1 GENERAL

1.1 Introduction

At A1 Telekom Austria Group ("**A1 Group**"), our core mission is to deliver reliable, high-quality telecommunication services and technology solutions to our customers. As an international telecommunications provider, we prioritise compliance with privacy laws and regulations, the safeguarding of Personal Data and assurance of network security which are fundamental to our operations. The adoption of this Personal Data Privacy and Protection Policy ("**Policy**") is a critical step in reinforcing our commitment to meeting these requirements.

Accordingly, this Policy reaffirms A1 Group's dedication to raising its Personal Data protection standards by establishing clear guidance on the secure, confidential, lawful and responsible processing of Personal Data in compliance with the applicable laws and international best practices.

Furthermore, this Policy implements a formal Data Privacy Program, which consists of a structured set of principles, policies, standards, guidelines, training mechanisms and controls designed to manage Personal Data across A1 Group in a secure and legally compliant way. The Policy also defines the roles and responsibilities of individuals and corporate bodies involved in Personal Data processing.

1.2 Purpose

The overall objective of this Policy is to ensure that A1 Group processes Personal Data in compliance with the applicable legislation and international standards. This Policy has been designed to provide A1 entities the required structure and guidance for incorporating appropriate standards and practices into their daily operations.

In particular, this Policy defines fundamental principles and guidelines governing the processing of Personal Data across all A1 entities and establishes the Data Privacy Program ensuring that Personal Data is handled securely and in accordance with applicable laws. Additionally, this Policy helps us to demonstrate our commitment to safeguarding Personal Data, which is crucial for maintaining trust with stakeholders and complying with legal obligations.

1.3 Scope

1.3.1 Personal Data

This Policy applies to the Personal Data processed by or on behalf of A1 Group entities in the capacity of a controller or processor.

1.3.2 Entities and People in Scope

This Policy, and all documents within the Data Privacy Program, apply to all companies of A1 Group except as specified in paragraph 1.3.3 below.

Additionally, we require all third parties, such as external suppliers, who have access to the Personal Data held by A1 Group to adhere to this Policy. The respective requirements are incorporated in the data processing agreements and other documentation exchanged with a third party. If such third party is unable to meet a specific requirement, we expect them to implement an alternative solution that achieves the same result as the original requirement.

This Policy is applicable to all employees of A1 Group. Every A1 employee has responsibility, within their work area, to ensure that Personal Data are collected, stored and handled in accordance with applicable laws.

1.3.3 Application of National Laws

This Personal Data Privacy and Protection Policy is based on the provisions of the privacy legislations in which we operate, including GDPR, and A1 Code of Conduct. This Policy includes the minimum standard to which all A1 companies in scope, employees and suppliers must adhere, regardless of whether the GDPR directly applies to their country or specific activity.

The relevant national laws of an A1 company will take precedence if there is a conflict with this Policy. This Policy must also be observed in the absence of corresponding national legislation or where national legislation has a lower standard.

2 DATA PRIVACY PROGRAM

2.1 General

The A1 Data Privacy Program ("**Program**") is a set of policies, guidelines, standards reflecting the actions we must take to comply with our legal obligations and demonstrate on an ongoing basis that we have implemented the necessary controls to protect Personal Data. The Program embraces principles, governance structure and controls which govern the processing of the Personal Data across A1 Group in a secure and legally compliant way.

2.2 Structure of the Program

The Program is documented in policies, guidelines and standards. These types of documents differ in the level of detail. Policies are more generic guidelines and standards are more specific. The documents are mandatory for the A1 entities and employees in scope except as specified in paragraph 1.3.3. We may also use handbooks including a set recommendations, best practices and templates which are not mandatory but represent the best practices within A1 Group. In addition, for policies, guidelines and standards there is a separation into the two target audiences: group level and local level.

The structure described above is visualised in **Figure 1**. The document types are described in more detail below, including target audience and examples of content. A1 companies may have different titles for below document's types (e.g. rulebooks, procedures, instructions).

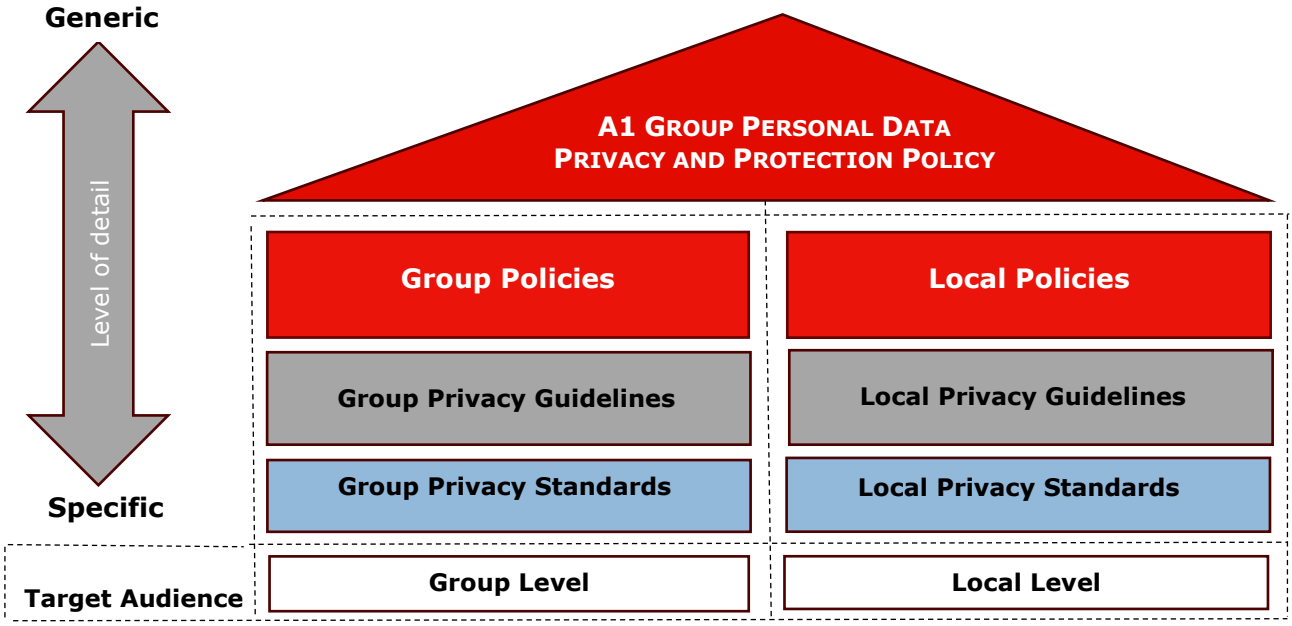

Figure 1: A1 Data Privacy Program

Doc ID: **PRI-POL-GRP-ENG-V**1.0
Effective date: 02.03.2026
A1 Classification: Public

2.2.1 A1 Group Personal Data Privacy and Protection Policy

This Policy is the highest document in the A1 Data Privacy Program. It outlines the A1 general data privacy strategy and governance system and must be considered as the main document alongside more detailed documents such as guidelines on specific topics of data processing activities. This Policy defines the objectives, guideline principles, governance structure, key roles and responsibilities in the data privacy domain at A1 Group. The Policy is a public document which is published for the general public.

The Data Protection Officer of Telekom Austria AG is responsible for maintaining the Policy.

We may introduce other policies on the Group or local level to cover specific topics in the data protection domain.

2.2.2 Group Data Privacy Guidelines

The middle tier of the Data Privacy Program includes specialised guidelines on various aspects of the processing of Personal Data. The guidelines detail the minimum requirements specified in this Policy and include mandatory requirements and optional recommendations in the subject areas relevant for data privacy on the A1 Group level.

2.2.3 Local Data Privacy Guidelines

In addition to the Group data privacy guidelines, the A1 entities in scope of this Policy can define stricter requirements or requirements in compliance with local laws in local data privacy guidelines. These requirements must only be met by the respective A1 entity and must not contradict or lower mandatory requirements of the A1 Group data privacy guidelines, unless it is necessary to comply with the local legislation.

2.2.4 Group and Local Privacy Standards

In A1 Group privacy standards, we define granular requirements and recommendations for the processing Personal Data. These requirements are binding but might not be applicable to all A1 entities.

If needed, in addition to A1 Group privacy standards, A1 entities have the authority to establish stricter or more specific requirements in local privacy standards that apply exclusively to their operations.

3 GOVERNANCE AND ORGANISATIONAL STRUCTURE

3.1 General information

To implement, execute and oversee the Data Privacy Program (including this Policy), A1 Group has established a governance structure comprising the upper management and A1 Group and local privacy teams with expertise in legal and operational data protection matters. All employees and corporate bodies involved in the data privacy domain are committed to ensuring that A1's data protection standards meet legal requirements while aligning with its commercial objectives.

Every A1 entity must have adequate data protection capabilities including dedicated personnel with sufficient resources and powers. Depending on the size and needs of the A1 entity this can be a dedicated data protection body, a Data Protection Officer ("**DPO**"), a supporting team (such as legal counsels and data protection coordinators) and/or a combination of these roles.

3.2 A1 Group Senior Management

The A1 Group CEO and the Group Management Board have overall responsibility for data protection and data governance in A1 Group. The A1 Group Management Board is responsible for the Group-wide decisions and approving this A1 Personal Data Privacy and Protection Policy and other Group-wide policies.

3.3 Local Senior Management

The local A1 company senior management teams ("**Local Leadership Team**") are responsible for data protection and governance in their respective A1 entities by ensuring compliance, allocating resources, fostering a culture of data security, and ultimately demonstrating commitment to protecting Personal Data. The Local Leadership Team should ensure that their local privacy function has sufficient resources and support to fulfil their duties.

3.4 A1 Group Privacy Function

A1 Group privacy function is responsible for the data privacy governance matters affecting A1 Group as a whole, in particular:

(a) Awareness of the new legislation in the privacy domain;

(b) Drafting and maintaining A1 Group policies and guidelines;

(c) A1 Group privacy risk management;

(d) General strategy questions;

(e) Coordinating A1 Group internal audits and compliance in relation to privacy matters.

3.5 A1 Group Privacy Team

A1 has a Privacy Team comprising the DPOs and other employees responsible for the data protection matters. The Privacy Team fulfils advisory, consultative, and coordination functions and may address the following matters:

(a) Operational topics such as data processing and data sharing agreements, ROPA, DPIA, PIA, LIA, Group projects;

(b) Risk management (risks in data privacy and internal privacy controls) and data privacy audit;

(c) Contribution to the specialised policies and guidelines on various aspects of the processing of Personal Data;

(d) Coordination of training, awareness and internal communication strategy;

(e) Strategy for the prevention of Personal Data breaches and for safeguarding the rights of Data Subjects.

3.6 Data Protection Officers

Each OpCo and, where applicable, other A1 entities must appoint one or more DPO. The DPOs are the internal and external contact people in the OpCo's for data protection matters. The Local Leadership Team is required to assist the DPOs with their efforts.

Within each OpCo the DPO will have to (i) operate independently; (ii) report to the local senior management of the OpCo, i.e. to the local CEO or management board; and (iii) be provided with adequate resources to enable the DPO to meet their obligations.

The main tasks of the DPO are to:

(a) Inform and advise the organisation and its employees about their obligations to comply with the applicable data protection laws and this Policy;

(b) Advise business units on data protection matters and implementation of the projects involving Personal Data (including DPIAs and PIAs);

(c) Monitor compliance with the data protection laws and conduct internal audits with the support and guidance of the A1 Group and local internal audit function;

(d) Assist the business units at maintaining a record of the data processing activities;

(e) Be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc.) and manage the inquiries of competent authorities with regard to the Personal Data;

(f) Prepare, review and, where appropriate, update any privacy notices as required by the applicable laws;

(g) Review, update and arrange execution of the data processing and data transfer and sharing agreements with third parties;

(h) Assist at data breach management and reporting; and

(i) Process in a timely manner the requests submitted by Data Subjects in connection with the exercise of their rights over their Personal Data and establish procedures to address their complaints.

In order to ensure compliance with the Data Privacy Program and local data protection laws, our DPOs established procedures for the periodic reporting to the senior management. This allows the senior managers to monitor privacy and Personal Data protection issues on an ongoing basis and the DPOs to raise their concerns to the upper management.

4 GUIDING PRINCIPLES

4.1 General Principles for Processing Personal Data

During our business activities, we collect Personal Data in different ways through various channels. We may process a variety of Personal Data depending on the nature of the services, including, without limitation, identification or authentication, contact, financial, fiscal, tax, demographic data, information about the devices used for the provision of our services and the geographic location of such devices, information about the Data Subject's interests and preferences with respect to our services.

In compliance with applicable laws, A1 Group adheres to the following basic principles when collecting and processing the above Personal Data and entrusting external vendors to process Personal Data on its behalf. All data processing activities, irrespective of their location, must be guided by these principles to ensure the responsible handling of Personal Data. The Personal Data must be:

1. Processed **lawfully, fairly and in a transparent manner**.

2. Collected and processed for **specified, explicit and legitimate purposes** and in an appropriate way.

3. **Adequate, relevant, and limited** to what is necessary in relation to the purposes for which they are processed.

4. **Accurate** and, where necessary, **kept up to date**.

5. Retained for the time that is **necessary for the specified purposes** except for the situation permitted by law.

6. Processed in a manner that ensures **appropriate security and confidentiality**.

7. Not transferred to countries without **adequate protection** of the Personal Data.

4.2 Lawfulness, Fairness and Transparency

4.2.1 Lawfulness

The Personal Data must be processed and collected lawfully, fairly and in a transparent manner in relation to the Data Subject in compliance with applicable laws. For our processing activities to be lawful, processing of Personal Data must be based on an appropriate legal basis. Furthermore, Data Subjects must be informed of how their data are being handled, usually in the form of a privacy policy or statement.

4.2.2 Legal Grounds for Data Processing

A lawful legal basis under applicable law is necessary to collect and process Personal Data. The choice of an appropriate legal basis depends on the legal applicable legal requirements, purpose of processing and relationship with the individual.

If the original purpose for collecting and processing Personal Data is to be changed, the Controller must consider whether it needs another legal basis or make a compatibility assessment in relation to the original purpose and the new purpose.

4.2.3 Transparency

Prior to collecting Personal Data we must inform Data Subjects, in a fair and transparent manner, using clear and plain language, at least of the following:

(a) the legal person responsible for processing Personal Data;

(b) types of Personal Data collected from the Data Subjects;

(c) permitted uses of Personal Data;

(d) information about transfer of personal data to third jurisdictions.

We may use automated decision-making ("**ADM**") processes and AI-driven algorithms to analyse consumer preferences, forecast trends, and improve our products and services. These technologies will be deployed ethically, ensuring fairness, respect for individual rights, and non-

discrimination. Where required by law, we will disclose relevant information related to the adoption of ADM processes and AI-based algorithms.

4.3 Purpose Limitation

The Personal Data must be collected and processed for specific and explicit purposes which the Data Subject has authorised except as permitted by applicable laws. The Data Subjects must be informed about the primary and secondary purposes for which Personal Data will be handled.

We may collect the Personal Data for various purposes depending on the type of data, the services we provide and the context within which we collected such data. Subsequent changes to the purpose are only allowed to a limited extent and may require a new lawful basis.

4.4 Data Minimisation

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed. In any processing of Personal Data, we will endeavour to process and limit the collection of Personal Data to the minimum necessary in relation to the purposes for which they are sought. Accordingly, we will make efforts to avoid processing Personal Data that is excessive and/or is not relevant to the purposes for which they are processed.

When possible, we will anonymise Personal Data to reduce the risk of unlawful processing. Once data is anonymised in a way that prevents individual identification, data protection laws no longer apply.

4.5 Accuracy

Personal Data must be accurate and up to date. We will take every reasonable step to ensure that inaccurate Personal Data are deleted or rectified, having regard for the purpose for which they are processed.

4.6 Retention of Personal Data

Personal Data must be retained only for as long as necessary to fulfil the purposes for which it was collected or processed. In certain cases, retention may be required beyond this period when justified by legal, regulatory, or contractual obligations. Once the applicable retention period expires, we will ensure the secure and permanent deletion or anonymisation of Personal Data to prevent unauthorised access or misuse.

4.7 Security and Confidentiality

4.7.1 Personal Data Security

Personal Data must be processed in a manner that ensures appropriate security and prevention of unauthorised access, disclosure, dissemination or manipulation. A1 Group is committed to ensure, through the implementation of technical and organizational measures, the ongoing integrity, availability and confidentiality of Personal Data in accordance with the requirements set forth in the applicable laws and international best practices.

We continuously monitor the performance of our systems, applications, and technological infrastructure to ensure that privacy and data protection remain at the highest standards.

However, despite these precautions, certain incidents may compromise the security and confidentiality of Personal Data. In such cases, we will respond in accordance with our security incident management procedure and any other relevant internal policies or procedures depending on the jurisdiction where such incident took place. Furthermore, where legally required, we will

notify the affected individuals and/or the appropriate supervisory authorities of the Personal Data Breach.

4.7.2 Confidentiality

Personal Data is confidential, and unauthorised collection and processing of Personal Data is strictly prohibited. All A1 Group employees are required to understand and adhere to the security and confidentiality measures.

Employees may only access Personal Data if necessary for their legitimate duties, following the need-to-know principle. Roles and responsibilities must be clearly defined, with access rights appropriately limited.

A1 employees must not use Personal Data for personal or commercial purposes, share it with unauthorised individuals, or disclose it in any form. Supervisors must inform employees of their data secrecy and confidentiality obligations at the start of employment, and these obligations continue even after employment ends.

4.8 Transfers of Personal Data

Any transfer of Personal Data to recipients outside and inside of A1 Group is subject to data protection laws and internal A1 Group requirements.

The Personal Data must not be transferred to the countries that do not offer an adequate level of protection of Personal Data as well as safeguards for the fundamental rights and freedoms of the Data Subjects. Any transfer and/or transmission of Personal Data shall be carried out in accordance with a legally binding instrument that sets forth the parties' obligations with respect to the protection of such data under the laws of the relevant country.

Where feasible and required by law, we will inform the Data Subjects about the recipients or types of recipients and the purposes for which the information will be transferred.

4.9 Privacy by Default and Privacy by Design

We endeavour to implement "Privacy by Design" and "Privacy by Default" approaches which ensure Personal Data protection is embedded into systems and processes from the outset. This means that data protection measures are integrated into the development of products, services, and business processes from the very beginning rather than as an afterthought ("**Privacy by Design**") and it is ensured that, by default, only the minimum necessary personal data is collected, processed, and shared ("**Privacy by Default**").

We follow this approach in all our work, but in particular when:

(a) building new IT systems for storing or accessing Personal Data;

(b) developing new applications or new use cases for existing systems;

(c) embarking on a data sharing initiative; or

(d) using Personal Data for different purpose(s) than for which they had been collected.

4.10 Privacy of Communications

Protecting the privacy of our customers' communications is a fundamental principle at A1 Group, upheld not only as a legal obligation, but also as a responsibility to maintain public trust. We are committed to make sure that no one may intercept, monitor, or disclose any communication

without a legally justified, written order from a competent authority. The delivery of information to competent authorities is only allowed where required in accordance with the requirements set forth in the applicable laws of each of the countries in which we operate.

4.11 Requests of Competent Authorities

The OpCos engaged in telecommunications services must, as holders of telecommunications concessions or licences, comply with national security and law enforcement requirements.

In any such case, we will thoroughly review and analyse the relevant request in order to comply with the law, ensure that human rights are respected and notify the Data Subject about such requests, where legally permitted. However, not all the jurisdictions in which we operate offer harmonised protections against the government's access to the Personal Data. Hence, in certain cases we will be required by law to cooperate with the government in matters pertaining to security and law enforcement without prior notice to the Data Subjects.

5 RIGHTS OF THE DATA SUBJECTS

5.1 Data Subject Rights

The Data Subjects have the full scope of rights towards any A1 entity under the data protection laws in each jurisdiction in which such entity operates. In particular, the Data Subject has the following minimum rights:

(a) **Right to be informed:** The Data Subjects have the right to know how their Personal Data is collected, used, and processed. A1 entities must provide clear and transparent privacy notices outlining this information.

(b) **Right of access**: The Data Subjects can request access to their Personal Data, including details on how it is processed, who has access to it, and for what purpose.

(c) **Right to rectification**: The Data Subject can request corrections to inaccurate or incomplete Personal Data without undue delay.

(d) **Right to erasure**: The Data Subject may request their Personal Data to be deleted under certain conditions such as when the processing of such data is no longer necessary, or consent is withdrawn.

(e) **Right to restrict processing:** The Data Subject can request that their Personal Data processing be limited (e.g., if data accuracy is disputed or processing is unlawful, but the individual does not want the data deleted).

(f) **Right to data portability**. The Data Subject has the right to request that the Personal Data held by A1 are provided to him/her and in a structured, commonly used, and machine-readable format.

(g) **Right to object**: The Data Subject generally has a right to object to the processing of their Personal Data, especially for direct marketing or processing based on legitimate interests or public interest.

(h) **Rights Related to Automated Decision-Making and Profiling**: The Data Subject has the right not to be subject to decisions based solely on automated processing, including profiling, if these produce legal effect concerning him or her or otherwise significantly affect them, unless specific legal conditions are met.

(i) **Right to Lodge a Complaint**: Individuals can file complaints with the relevant supervisory authority if they believe their rights have been violated.

(j) **Right to Withdraw Consent**: Where data processing is based on consent, Data Subjects can withdraw their consent at any time.

6 PRIVACY RISK OVERSIGHT AND ASSESSMENT

6.1 General

The identification, assessment, and management of privacy risks are fundamental components of the A1 Group's overall risk management and accountability framework. A thorough understanding of the risks involved in processing Personal Data is crucial for objectively evaluating potential threats and determining effective mitigation measures. A1 Group adopts a systematic and proactive approach to address privacy risks, which includes conducting privacy risk assessments, implementing both internal and external audit controls, and continuously monitoring and reviewing data processing activities.

Each A1 entity may implement additional processes for privacy risk analysis when required by applicable local legislation. Such local requirements do not limit or replace the obligations defined in this Policy.

6.2 Internal Control System

A1 Group companies are subject to the requirements of the Framework for Internal Control Systems in Austria & CEE Segment of América Móvil ("**ICS Framework**"). In compliance with the ICS Framework, we have developed the Internal Control System for Data Privacy ("**Privacy ICS**") to identify the main risks in the A1 Group Personal Data processing activities and to manage and mitigate such risks.

6.3 Audit

6.3.1 Internal Audit

According to the Austrian Code of Corporate Governance, an internal audit department, the Group Internal Audit ("**GIA**") is established on the A1 Group level. The GIA department reports to the Audit Committee of the Supervisory Board of Telekom Austria AG at least annually. The activities of the GIA are governed by the Group Internal Audit Charter (internal document) and include regular and *ad hoc* audits of the adequacy and effectiveness of the data protection and data processing activities within A1 Group.

The A1 entities may also conduct local internal audits to review the data protection and data processing activities in the relevant jurisdictions.

6.3.2 External Audit

We also arrange, on *ad hoc* basis, external data protection and data governance audits to review our data protection practices, systems and processes. The auditors may also assess our organisation's privacy governance structure, training and awareness programs, and Personal Data Breach response preparedness and risks management.

6.4 Compliance Risk Assessment

A1 Group has implemented a strong compliance management system ("**CMS**") in line with best practice of ESG and corporate governance standards. To maintain a best-practice CMS, we conduct an annual Compliance Risk Assessment ("**CRA**") and implement additional risk mitigating measures where required.

Our compliance and privacy teams will perform, at least annually, a yearly CRA on the Group level to determine the degree to which each A1 entity's systems, operations, processes and individuals are in compliance with applicable laws, our privacy policies and practices.

Please refer to the A1 Compliance Management System page for more information.

6.5 Data Protection Impact Assessment

Where required by the applicable laws in the jurisdictions in which we operate, A1 entities shall, prior to the processing, carry out a privacy impact assessment ("**PIA**") or data protection impact assessment ("**DPIA**"). As a general rule, we undertake a DPIA where a data processing operation is likely to result in a high risk to the rights and freedoms of Data Subjects. In addition, we use PIAs as a tool to evaluate privacy risks in various operational matters.

6.6 Record of Processing Activities

We will maintain at all times a comprehensive Record of Processing Activities ("**RoPA**") in accordance with applicable data protection laws and regulations, including the GDPR. This record will document all Personal Data processing activities conducted by A1 entities, ensuring transparency, accountability, and legal compliance. The RoPA will be regularly reviewed and updated to reflect any changes in processing operations.

7 PERSONAL DATA BREACH NOTIFICATION PROCESS

In the event of a Personal Data Breach, we are committed to handling the situation with utmost care and transparency. A Personal Data Breach occurs when there is unauthorised access to, disclosure of, or loss of Personal Data. If such an incident occurs, we will promptly assess the breach to determine its severity and impact on affected individuals. We will notify the relevant data protection authorities and, where required by law, inform the individuals whose Personal Data has been compromised.

Personal Data Breaches often result from IT security breaches, though not each security breach will necessarily be a Personal Data Breach. For this reason, A1 entities implement a robust security incident management process and reporting lines between security and privacy teams to manage potential consequences of security incidents which may lead to a Personal Data Breach.

8 TRAINING AND AWARENESS

At A1 Group, it is essential that all employees and external workforce not only understand but actively apply the principles outlined in this Policy. To foster a culture of transparency, ethics, and strong values, we provide both online and in-person training programs. These courses, announced through official company communication channels, are designed to ensure a clear understanding of key concepts, responsibilities, and real-world course of action in the data privacy domain.

9 SUPERVISION AND POLICY COMPLIANCE

The implementation and compliance with the Data Privacy Program, including this Policy, is embedded into our A1 Group-wide risk and compliance management system. The A1 Group compliance function, the compliance function of the A1 companies and the GIA are those responsible, within their competence, for supervising and periodical auditing the due compliance of the provisions indicated in this Policy.

The local privacy team is responsible for day-to-day compliance and periodical evaluation of the Data Privacy Program, including this Policy. Likewise, they are responsible for educating the employees regarding this Policy.

It is everyone's obligation to comply with this Policy and report any act that is against it, through the whistleblowing portal.

10 PENALTIES

The penalties for violation of this Policy and/or data protection laws, both for the A1 employees and third parties, may be of administrative, labour, or even criminal kind, depending on the seriousness of the act, and they shall be sanctioned according to the internal work regulation and/or according to the applicable law. In particular, the consequences may include fines to A1 entities, disciplinary actions and termination of employment for employees or termination of business relationship with third parties.

11 APPENDICES

11.1 Appendix A – Terms and Abbreviations

Term	Definition
A1 Group	means Telekom Austria Group (TAG) consisting of Telekom Austria AG, registered under FN 144477t at the Commercial Court of Vienna and all companies worldwide in which Telekom Austria AG holds a direct or indirect interest of at least 50%;
Controller	means the legal person that determines the purposes and means of the Processing of Personal Data;
Data Subject	means the natural person to whom certain Personal Data relate;
DPIA	means a process designed to identify risks arising out of the processing of personal data and to minimise these risks for data processing activities that may result in a high risk to the rights and freedoms of the data subject such as processing sensitive data;
ESG	stands for Environmental, Social, and Governance and represents a framework used to evaluate an organization's sustainability and ethical impact;
GDPR	means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016;
Data Privacy Program	means a set of policies, guidelines, standards reflecting the actions we must take to comply with our legal obligations and demonstrate on an ongoing basis that we have implemented the necessary controls to protect Personal Data;
"**Operational Company**" or "**OpCo**"	means any legal entity of A1 Group which has a telecommunication licence in the respective territory;
Personal Data	means any information concerning an identified or identifiable individual;
Personal Data Breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
Privacy ICS	means the Internal Control System for Data Privacy designed to identify the main risks in Personal Data processing activities and to mitigate such risks;
Processor	means a natural or legal person that, alone or jointly with others, processes Personal Data on behalf of controller;
Processing	means the collection, use, disclosure or storage of Personal Data by any means. Use includes any action of access, management, exploitation, transfer or disposal of Personal Data;

Supervisory Authority	means the relevant supervisory authority with responsibility for privacy or data protection matters in the jurisdiction of A1 company;
PIA	means a process used to identify and assess potential privacy risks associated with a project, program, or system with a view to ensure compliance with privacy laws and regulations.

12 REVISION AND UPDATES

All changes to this Policy, as well as the date on which such change(s) will come into effect, must be disclosed to the Data Subjects by means of an update notice posted in our relevant website(s).

The current and valid version of this document is available on A1 Group Data Privacy portal.

12.1 Version History

Version	Date	Author	Approved by	Approval date
1.0	02.03.2026	A1 Group Legal and General Counsel	A1 Group DPO	17.02.2026
	Initial release			

13 CONTACTS AND COMMENTS

Should you have any question related to this Policy or some comment or suggestion, please contact us at dataprotection@a1.group.