A1 Telekom Austria Group

Group Data Privacy Governance

March 22, 2019

Policy Section: Public **Handbook Section**: Internal

Approved by: Mag.a Judith Leschanz

Elaborated by: J.D. Daniel Sánchez Cordero Canela

1.0

A1 Telekom Austria Group Digital Declaration

We believe that enabling a positive and people-centered digital future requires constructive collaboration between stakeholders. Governments, industry and international organizations all have a stake in the digital future. Here we set forth our vision of the digital future we want, identifying the common set of outcomes we all strive for. Our vision for the digital future is one of:

Participation
Where the possibility of connectivity and digital technologies is extended to everyone, and where the development of digital capabilities is an integral part of every citizen's education.

Dynamic Digital Society

In which digital platforms, products, services and ecosystems delivered by a plethora of companies and technologies continue to advance and innovate, bringing about incalculable benefits and value to society.

Sustainable Digital Ecosystem

In which the digital ecosystem is enabled and empowered by supportive business and policy environments, capable of adapting with the speed of change of data-driven markets.

Digital Conduct

Where the internet is open, accessible and based on multi-stakeholder governance and cooperation and where online harassment and attempts outside the scope of relevant laws to restrict freedom of expression or access to information are opposed.

Privacy and Data

Where the privacy of digital citizens' is respected and their data handled in responsible, secure and transparent ways by all participants in the ecosystem, including providing consumers with opportunities to exercise choice and control over their data, whilst enabling innovation and other societal benefits.

Cybersecurity

Where all relevant stakeholders cooperate to mitigate cybersecurity threats and challenges to make people's digital experiences safe and secure.

Responsibilities

Where responsibilities and accountability for supporting and delivering a positive digital future are shared by all and policies, applied evenly across the digital landscape, are designed to realize specific goals, foster innovation and investment and benefit consumers.

Cooperation and Dialogue

Where constructive collaboration and dialogue between all stakeholders across geographies and industries enable further development of the promise of the digital future.

Big Data Analytics

Big data analytics and data driven services play a critical role in digital life and will continue to do so in the future. By using big data analytics to enhance connected cars, smarter homes, smarter cities and smarter health systems, we can have a positive impact on societal aims such as the UN Sustainable Development Goals and deliver more effective health outcomes, better environmental management, increased opportunities for learning and improved goods and services for consumers. In short, big data analytics changes the way we live – for the better. We have adopted a "privacy-by-design" ethos or methodology by which privacy and security safeguards are considered and designed into products, services, processes or projects at each stage of the lifecycle from cradle to grave.

A1 Telekom Austria Group and the United Nations Sustainability Development Goals

The way the world conducts business is changing. In addition to delivering financial performance and shareholder returns, we are also increasingly measured on the contribution we make to society. Investors, customers and employees now focus on our value to society and our ability to respond to the challenges facing the world. As we enter a fourth industrial revolution, social responsibility must be central to how we do business.

The Sustainable Development Goals (the "SDG") are the blueprint to achieve a better and more sustainable future for all. They address the global challenges we face, including those related to poverty, inequality, climate, environmental degradation, prosperity, and peace and justice. Multi-stakeholder partnerships, involving government, the private sector and civil society, have been described as the "glue" that will hold this process together, and will be the only way of ensuring these very goals are met.

We in Telekom Austria Group welcome the United Nations Sustainable Development Goals and will support the efforts in meeting such goals. We recognize that digital solutions can help drive the Sustainable Development Goals in the regions in which we operate and we are looking forward to contributing in order to ensure these goals are met. For example, by implementing digital solutions such as IoT/sensors, big data analytics, and cloud-based platforms, we can build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation.

Our customers are sending a very clear signal that they will shun companies that neglect or ignore their responsibilities to the communities in which they live and work. We demonstrate via our Group Data Privacy Governance that we rise to the challenge while at the same time protect the privacy of our customers, business partners and employees.

Objective of our Group Data Privacy Governance

Awareness
The Group Data Privacy Governance (the "Data Privacy Governance") intends to assist the management and employees of A1 Telekom Austria Group in the area of data protection and to raise awareness regarding the specificities of data protection regulation, particularly Regulation (EU) 2016/679 (the "GDPR").

Individual Responsibility
Even though our Data Privacy Governance is binding on all undertakings of A1 Telekom Austria Group, it does not impose any additional obligations which are already contemplated by regulation or law. Each undertaking of A1 Telekom Austria Group has the responsibility to comply with their own data protection regulations, as well as to meet the requirements set forth by the corresponding authorities.

Structure
Our Data Privacy Governance will be composed of a Policy and a Handbook. The Policy will be made public whereas the Handbook is for internal use only. The Handbook also contains multiple Annexes that are in the forms of questionnaires, checklists and templates, among other forms, which constitute best practices among A1 Telekom Austria Group and will help supplement compliance made by each undertaking of A1 Telekom Austria Group.

Minimizing Risk
Our Data Privacy Governance provides guidance on the implementation of appropriate measures and on the demonstration of GDPR compliance by A1 Telekom Austria Group. Based on Recital 77 of the GDPR, it serves as a self-regulating mechanism since they are indications provided by a data protection officer. However, each undertaking of A1 Telekom Austria Group is a risk-taker. Each undertaking of A1 Telekom Austria Group has to follow the recommendations and best practices contained herein. Each individual undertaking of A1 Telekom Austria Group can enrich the content according to their own local compliance assessments. It is to be noted that GDPR compliance is an ongoing process, developed on a constant basis in alignment with various business process. By incorporating our Data Privacy Governance the undertakings of A1 Telekom Austria Group are complying with their fiduciary duty of care. Furthermore, the Handbook section will be updated on a good faith basis to reflect changes in the legal framework in which A1 Telekom Austria Group operates.

Disclaimer
The content of our Data Privacy Governance is based on (i) the statutes and recitals of the GDPR, (ii) the content of various other legal regulations concerning data protection from European Union to Local level, (iii) European Court of Justice case-law, (iv) Guidelines, Opinions, Working Documents, and other forms of publications emitted by Article 29 Data Protection Working Party (now the European Data Protection Board) (v) Communications from the EU Commission, (vii) the Handbook on European Data Protection Law by the European Union Agency for Fundamental Rights and (vi) communications, guidelines, opinions and other forms of publications emitted by Data Protection Authorities throughout the EU.

The positions taken by A1 Telekom Austria Group in our Data Privacy Governance do not consists in affirmative statements of material fact or statements that would correspond to any type of liability should they be followed by third parties.

The Handbook section of our Data Privacy Governance may be amended in a good faith basis when there is new information available. Therefore, the Handbook is a "living" document.

Telekom Austria AG board has approved our Group Data Privacy Governance.

Vienna, March 22, 2019

Thomas Arnoldner
Chief Executive Officer
Telekom Austria AG

Alejandro Plater
Chief Operation Officer
Telekom Austria AG

Siegfried Mayrhofer
Chief Financial Officer
Telekom Austria AG

Group Data Privacy Governance Policy

March 22, 2019

Policy Section: Public **Handbook Section**: Internal

Approved by: Mag.a Judith Leschanz

Elaborated by: J.D. Daniel Sánchez Cordero Canela

1.0

1 Preamble

As a group of undertakings operating in an international capacity, it is of particular importance to meet the expectations of customers, business partners and employees in the confident, safe, and sensitive handling of their personal data.

Therefore, these two principles are valid for us:

- We effectively implement the laws and regulations of data privacy.
- We are oriented towards international standards of information security.

In providing the Data Privacy Governance, A1 Telekom Austria Group is delivering a standardized approach to the implementation needs regarding the GDPR, as well as various other regulations dealing with data protection. We implement our Data Privacy Governance as technical and organizational measures to ensure and to be able to demonstrate that processing of A1 Telekom Austria Group is performed in accordance with the GDPR and data protection regulations in the countries in which we operate. It is important to note that the legal system is dynamic and is subject to constant changes. However, by incorporating our Data Privacy Governance the undertakings of A1 Telekom Austria Group are complying with their fiduciary duty of care. In addition, as highlighted in the objectives of our Data Privacy Governance, A1 Telekom Austria Group will implement corresponding changes to the Handbook on a good faith effort to reflect the current framework of the regulations in which we operate.

Our Data Privacy Governance provides us with a self-regulating mechanism deemed to be evidence of compliance when we act as either controller or processor, especially as regards the identification of the risk related to the processing, their assessment in terms of origin, nature, likelihood and severity, and the identification of best practices to mitigate the risk of non-compliance. These measures, contained in the Handbook, will be reviewed and updated regularly based on new information available.

The due adoption by the undertakings of A1 Telekom Austria Group of the content and best practices mentioned in the Policy and in the Handbook will help to fulfil the implementation needs, as well as serve to demonstrate compliance with the GDPR. Our Data Privacy Governance is the combined result of requirements and interpretations regarding the successful EU-wide implementation of the GDPR, as well as various other regulations related to data protection. Our Data Privacy Governance shall be binding with regard to the processing of personal data for all A1 Telekom Austria Group. However, our Data Privacy Governance shall not impose any additional obligations which are already contemplated by regulation.

However, in light of other frame conditions not yet defined like the announced guidelines of the Article 29 Data Protection Working Party (now the European Data Protection Board), our Data Privacy Governance reflect the current state of interpretation of A1 Telekom Austria Group. It will be adopted in line with the further evolving of official statements and interpretations. Therefore, the Handbook will consists in a living document.

2 Objective

The protection of natural persons in relation to the processing of personal data is a fundamental right. The processing of personal data should be designed to serve mankind. § 8(i) of the Charter of Fundamental Rights of the European Union and § 16(i) of the Treaty on the Functioning of the European Union provide that everyone has the right to the protection of personal data concerning him or her.

The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. Everyone has, especially with respect to his private and to his family life, the right of confidentiality of their personal data. Customers, business partners and employees trust that we handle their data carefully.

Being a leading provider of digital services and communications solutions in Central and Eastern Europe with more than 24 million customers, currently operating in seven countries, the reputation and image of A1 Telekom Austria Group are particularly dependent on a legally compliant and secure handling of all personal data. The types of personal data that we process include, among others, contract data, traffic data, location data and employee data.

Recognising our aim to ensure data protection throughout A1 Telekom Austria Group the new General Data Protection Regulation (GDPR) will provide the legal and harmonized basis for all member of European Union (EU) and the European Economic Area (EEA) states and it will apply to any entity offering goods or services to (regardless of payment being taken) and any entity monitoring the behaviours of citizens within the EU and EEA.

It is of particular importance to highlight that A1 Telekom Austria Group subsidiaries do not constitute an undertaking as defined under § 101 and 102 of the Treaty of the Functioning of the European Union. Neither this Policy and Handbook, nor any other handbooks, directives, guidelines, policies, or working papers, warrants Telekom Austria AG, the ability to exercise decisive influence over the conduct of any of our subsidiaries.

3 Scope

This Policy is binding for all employees of A1 Telekom Austria Group when the material and territorial scope of the GDPR applies. It is enacted with approval from the board and its publication. It applies to the handling of all personal data, in particular data from customers, business partners and employees.

4 Data Privacy Strategy and Mission Statement

Our data privacy strategy and mission statement consists in the design and execution of technical and organizational measures in an efficient, risk minimizing and customer friendly manner to build digital trust for our customers, to secure brand value and to enable sustainable revenue growth by customer campaigning, advanced profiling and data monetization, in compliance with data protection regulations among the countries in which we operate.

5 Principles relating to Processing of Personal Data

The processing of personal data is only permitted if all of the following principles are met:

- Principle of lawfulness, fairness and transparency. Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.
- Principle of purpose limitation. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

- Principle of data minimization. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Principle of accuracy. Personal data shall be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Principle of storage limitation. Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- Principle of integrity and confidence. Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.
- Principle of accountability. We are responsible for, and are able to demonstrate compliance with all the above principles.

6 Lawfulness of Processing

The processing of personal data is only permitted if at least one of the following conditions is met:

- Consent. The data subject has given consent to the processing of his or her personal data for one or more specific purposes.
- Necessity for the performance of a contract. Processing of personal data is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
- Necessity for compliance with legal obligation. Processing of personal data is necessary for compliance with a legal obligation to which we are subject.
- Protection of vital interests. Processing of personal data is necessary in order to protect the vital interests of the data subject or of another natural person.
- Necessity for public interest or exercise of official authority. Processing of personal data is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in us.
- Legitimate interest. Processing of personal data is necessary for the purposes of the legitimate interests pursued by us or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

7 Processing of Sensitive Data

The processing of Sensitive Data is only permitted if at least one of the following conditions is met:

- Explicit consent. The data subject has given explicit consent to the processing of sensitive data for one or more specified purposes.
- Necessity for obligations in the field of employment and social security and social protection. Processing sensitive data is necessary for the purposes of carrying out

the obligations and exercising specific rights of us or of the data subject in the field of employment and social security and social protection law.

- Protection of vital interests. Processing sensitive data is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.
- Public. Processing sensitive data relates to personal data which are manifestly made public by the data subject.
- Necessity for legal claims. Processing sensitive data is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.
- Necessity for substantial public interest. Processing sensitive data is necessary for reasons of substantial public interest.
- Necessity for public interest, scientific or historical research or statistical purposes. Processing sensitive data is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

8 Data Protection Impact Assessment

A Data protection impact assessment is a process that help us identify and minimise the data protection risks of a project. We implement data protection impact assessments for processing that is likely to result in a high risk to individuals. To assess the level of risk, we consider both the likelihood and the severity of any impact on individuals. The Data Protection Impact Assessment is regulated under § 35 of the GDPR et seqq. as well under local regulation.

9 Processor

Where a processing operation is to be carried out on behalf of us acting as Controller, then we still have the responsibility for data privacy.

Before carrying out a processing by a processor, we ensure that:

- The processor provides sufficient guarantees to implement appropriate technical and organizational measures and procedures in such a way that the processing complies with the law and our rules.
- The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to us. Obligatory rules for data privacy and information security, as well as audit rights shall be part of the contract. The processor shall act only on the instructions provided from us.

10 Transfer of Personal Data to Third Countries

The transfer of data to a third country, including accessing the data from a third country, is permitted if the data processing itself is lawful and an adequate level of protection is provided in the third country where the recipient of the data is established. These rules also apply to the onward data transfer within the third country or to a different third country and regardless of whether the transfer takes place between controller/controller or controller/processor. The lawfulness of the data processing means, that in case of commissioned data processing, in addition to the adequate level of data protection a data processing agreement is required.

11 Rights of the Data Subject

Each person (data subject) has the following rights regarding his or her personal data:

- The right to be informed. Individuals have the right to be informed about the collection and use of their personal data. We provide privacy information to individuals at the time we collect their personal data from them. The information we provide to individuals is concise, transparent, intelligible, easily accessible, and it uses clear and plain language.
- The right of access. Individuals have the right to access their personal data. Individuals can make a subject access request verbally or in writing. Individuals have the right to obtain the following from us: (i) confirmation that we are processing their personal data; (ii) a copy of their personal data; and (iii) other supplementary information. An individual is only entitled to their own personal data, and not to information relating to other individuals (unless the information is also about them or they are acting on behalf of someone).
- The right to rectification. Individuals have a right to have inaccurate personal data rectified. In addition, an individual may also be able to have incomplete personal data completed. An individual can make a request for rectification in writing. In certain circumstances we can refuse a request for rectification.
- The right to erasure. Individuals have a right to have personal data erased. Individuals can make a request for in writing. The right is not absolute and only applies in certain circumstances.
- The right to restrict processing. Individuals have the right to request the restriction or suppression of their personal data. This means that an individual can limit the way that we use their data. The right is not absolute and only applies in certain circumstances. When processing is restricted, we are permitted to store the personal data, but not use it. An individual can make a request for restriction in writing.
- The right to data portability. The right to data portability allows individuals to obtain and reuse their personal data from their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability. The right to data portability only applies when: (i) the lawful basis for processing this information is consent or for the performance of a contract; and (ii) we are carrying out the processing by automated means (i.e. excluding paper files).
- The right to object. Individuals have the right to object to the processing of their personal data in certain circumstances. Even where the right to object applies, we may be able to continue processing if we have a compelling reason for doing so. An individual can make an objection in writing.
- Rights in relation to automated decision making and profiling. Individuals have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. We can carry out this type of decision-making where the decision is: (i) necessary for the entry into or performance of a contract; or (ii) authorized by EU law or member state law which we are subject to; or (iii) based on the individual's explicit consent.

12 Contact and Questions

In case of any questions e.g. regarding interpretation, implementation issues, the relation to other legal provisions, in case of any deviation of this Policy or if you like to provide ideas or best practices please contact the GDPR team (dataprotection@a1.group).

Telekom Austria AG board has approved this Group Data Privacy Policy.

Vienna, March 22, 2019

Thomas Arnoldner
Chief Executive Officer
Telekom Austria AG

Alejandro Plater
Chief Operation Officer
Telekom Austria AG

Siegfried Mayrhofer
Chief Financial Officer
Telekom Austria AG