Data Processing Agreement in accordance with Article 28 General Data Protection Regulation (GDPR)

This Agreement is entered into by and between:

I. **Company of Telekom Austria Group (TAG)** – hereinafter referred to as "Controller";

II. **Supplier** – hereinafter referred to as "Processor";

each a "**Party**" and together the "**Parties**".

1. Subject and Duration of the Order or Contract

The Parties have entered into a Framework Agreement ("Agreement"). In the course of providing the services etc as defined in this Framework Agreement it may be necessary for the Processor to process certain data on behalf of the Controller, who may act as a "controller" or as a "processor" as defined under the Applicable Law. In addition to the Agreement, this contract shall apply in order to comply with the legal requirements on data protection. Unless otherwise agreed here, the provisions of the Agreement in force today shall remain unchanged.

2. Data Processing

2.1 Definitions

Applicable Law	shall mean the relevant data protection and privacy law (including GDPR) to which Controller is subject, and any guidance or codes of practice issued by the relevant Privacy Authority(ies);
Authorized Companies	shall mean any legal entity of A1 Telekom Austria Group which is permitted to use the Services, but has not signed its own Framework Agreement with the Processor;
General Data Protection Regulation (GDPR)	shall mean the Regulation (EU) 2016/679 coming into effect on May 25, 2018 according to which the Directive 95/46/EC is repealed;
Personal Data	shall mean any information relating to a natural person as defined by the Applicable Law and including the categories of data listed in the Processing Appendix (Schedule 2) together with any additional such personal data to which Processor have access from time to time in performing the Services under this Agreement;

Privacy Authority	shall mean the relevant supervisory authority with responsibility for privacy or data protection matters in the jurisdiction of a Controller;
Processing	shall mean any operation or set of operations which is performed on Personal Data, including collection, structuring, storage, adaption or alteration, retrieval, use, disclosure by transmission, dissemination or otherwise making available, erasure or destruction of Personal Data as defined by the Applicable Law;
Processing Appendix	shall mean each appendix in a format substantially as set out in Schedule 2, agreed by the parties and incorporated into Schedule 2 and subject to the terms of this Agreement as of the effective date specified therein;
Services	shall mean the services provided by the Processor in relation to the Processing of Personal Data as described in a Processing Appendix from time to time;
Standard Contractual Clauses	shall mean the clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (Schedule 1);

2.2 Information Security

(1) Processor shall keep Personal Data logically separate to data Processed on behalf of any other third party.

(2) Processor warrants that it maintains and shall continue to maintain appropriate and sufficient technical and organisational security measures to protect Personal Data against accidental, unlawful destruction or accidental loss, damage, alteration, unauthorised disclosure or access, in particular where the Processing involves the transmission of data over a network, and against all other unlawful forms of Processing.

(3) Processor assures to comply with the Information Security Requirements for Suppliers. The Information Security Requirements are available for viewing, printing and downloading under https://www.a1.digital/ueber-a1-digital/Lieferanteninformantionen-a1-digital

(4) The controller may unilaterally amend the Information Security Requirements if the amendment leads to a reduction in the duties of the processor or if the amendment is necessary to take account of legally provided requirements.

(5) In the event that any of the Personal Data is corrupted or lost or sufficiently degraded as a result of the Processor's negligence or default so as to be unusable then, in addition to any other remedies

that may be available to the Controller under this Agreement or otherwise, the Controller shall have the option to:

a. require the Processor at its own expense to restore or procure the restoration of the Personal Data and the Processor shall use all reasonable endeavours to do so as soon as possible; or

b. restore itself or procure the restoration of the Personal Data and require the Processor to reimburse the Controller for any reasonable costs incurred in so doing.

2.3 Processing of Personal Data

(1) The Processor warrants in respect of all Personal Data that it Processes on behalf of Controller, that:

a. it shall only Process such Personal Data for the purposes of providing the Services and as may subsequently be agreed by the parties in writing and, in so doing, shall act solely on the documented instructions of Controller, including instructions to refrain from further Processing.

b. it shall not itself exercise control, nor shall it transfer Personal Data to a third party, unless expressly specified otherwise by Controller;

c. it shall not Process, apply or use the Personal Data for any purpose other than as required and is necessary to provide the Services;

d. it shall not Process Personal Data for its own purposes or include Personal Data in any product or service offered to third parties.

(2) In order to ensure that Controller's instructions in respect of any Personal Data can be carried out as required under this Agreement, the Processor shall have in place appropriate processes and any associated technical measures, including the following:

a. The duty to assist Controller with regard to Controller's obligation to provide information to the individual data subject and to immediately provide Controller with all relevant information in this regard;

b. updating, amending or correcting the Personal Data of any data subject upon request of Controller from time to time;

c. cancelling or blocking access to any Personal Data upon receipt of instructions from Controller;

d. the flagging of Personal Data files or accounts to enable Controller to apply particular rules to individual data subjects' Personal Data, such as the suppression of marketing activity.

(3) The Processor shall comply with the Applicable Law and shall not perform its obligations under this Agreement in relation to the Personal Data in such a way as to cause Controller to breach any of their obligations under Applicable Law.

(4) The Processor shall give Controller such co-operation, assistance and information as Controller may reasonably request to enable it to comply with its obligations under any Applicable Law. Further, the Processor shall co-operate and comply with the directions or decisions of a relevant Privacy Authority.

(5) Prior to commencing the Processing, and any time thereafter, Processor shall promptly inform Controller if, in its opinion, an instruction from Controller infringes any Applicable Law.

(6) The parties acknowledge and agree that Processor shall not be entitled for reimbursement of any costs, which Processor may incur as a result of or in connection with complying with Controller's instructions for the purposes of providing the Services and/or with any of its obligations under this Agreement or any Applicable Law.

(7) The Processor shall maintain a written record of all categories of Processing activities carried out on behalf of the Controller (the "Record") as defined in the Applicable Law and shall provide such Record to Controller within five (5) working days upon Controller's written request.

(8) Data Protection Officer/Representative: The Processor and Controller shall comply with the legal requirements to appoint a Data Protection Officer and/or nominate a Representative pursuant to Article 27 para 1 GDPR. The Parties shall give each other written notice in case of any change of the Representative.

3. Processing of Personal Data outside of the EEA

Where Personal Data originating in the European Economic Area is Processed by the Processor outside the European Economic Area or in a territory that has not been designated by the European Commission as ensuring an adequate level of protection pursuant to Applicable Law, the Processor and Controller agree that the transfer will be subject to the Standard Contractual Clauses which shall be deemed to apply in respect of such Processing.

The Processor shall ensure that the Processing of such Personal Data does not commence until Controller has confirmed to the Processor that it has obtained any approvals required from relevant Privacy Authorities.

4. Data Breach and Notification Requirements

(1) Processor shall immediately, but not later than 20 hours, inform Controller after becoming aware of any accidental, unauthorized, or unlawful destruction, loss, alteration, or disclosure of, or access to, Personal Data ("Security Breach").

(2) Such notification shall at least include all elements as defined in Article 33 para 3. and additionally in such notification or thereafter as soon as such information can be collected or otherwise becomes available, any other information Controller may reasonably request relating to the Security Breach.

(3) The Processor shall take immediate action to investigate the Security Breach and to identify, prevent and make best efforts to mitigate the effects of any such Security Breach in accordance with its obligations under this Clause and, subject to Controller's prior agreement, to carry out any recovery or other action necessary to remedy the Security Breach.

(4) The Processor shall not release or publish any communication, notice, press release, or report concerning any Security Breach in respect of Personal Data ("Notices") without Controller's prior written approval.

(5) The actions and steps described in this Clause shall, without prejudice to Controller's right to seek any legal remedy as a result of the breach, be undertaken at the expense of the Processor and the Processor shall pay for or reimburse Controller for all costs, losses and expenses relating to the cost of preparing and publishing Notices.

(6) In the event the Security Breach will impact more Processor's customers, Processor shall prioritize Controller in providing support and implement necessary actions and remedies.

5. Processor Employees – Confidentiality

(1) The Processor shall ensure the reliability of any employees and Subprocessors personnel who access the Personal Data and ensure that such personnel have undergone appropriate training in the care, protection and handling of Personal Data and have entered into confidentiality provisions in relation to the Processing of Personal Data that are no less onerous than those found in the Framework Agreement.

(2) Processor will remain liable for any disclosure of Personal Data by each such person as if it had made such disclosure.

6. Subcontracting

For the purposes of this clause, subcontracting shall mean services which are directly related to the provision of the services referred to in Schedule 2.

This does not include ancillary services which the Processor uses, e.g. as telecommunications services, postal/transport services, user services or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems. The Processor is, however, obliged to take appropriate and legally compliant contractual agreements and control measures to ensure data protection and data security of Controller's data, even in the case of outsourced ancillary services.

(1) Processor is not allowed to sub-contract or outsource any Processing of Personal Data to any other person or entity, including its affiliated companies ("Subprocessor") unless and until:

a. The Processor submits such a sub-contracting or outsourcing to a Subprocessor to Controller in writing with an appropriate advance notice (not less than 180 days) including all information such as

   i. name and registered office or principal place of business of the Subprocessor;

   ii. details (including categories) of the processing to be carried out by the Subprocessor in relation to the Services;

   iii. and such other information as may be requested by Controller in order for Controller to comply with Applicable Law, including notifying the relevant Privacy Authority.

b. Processor has made legally binding contractual agreements no less onerous than those contained in this Agreement on such Subprocessor;

c. Processor has entered into Standard Contractual Clauses, Module 3, "Transfer processor to processor", with the sub-contracting third party, if and to the extent the scope of sub-contracting involves the transfer of Controller's Personal Data to, the storage of Controller's Personal Data in or the Processing of Controller's Personal Data by any other means in third countries without an adequate level of protection as determined by an adequacy decision of the EU Commission.

(2) Where requested by Controller, Processor shall procure that any third party Subprocessor appointed by Processor pursuant to this clause shall enter into a data processing agreement with Controller on substantially the same terms as this Agreement.

(3) In all cases, Processor shall remain fully liable to Controller for any act or omission performed by Subprocessor or any other third party appointed by it as if they were the acts or omissions of the Processor.

(4) In the event of a breach of this Agreement caused by the actions of a Subprocessor, the Processor shall – if requested by Controller - assign the right to Controller to take action under the Processor's contract with the Subprocessor as it deems necessary in order to protect and safeguard Personal Data.

7. Security of Communications

(1) The Processor shall undertake appropriate technical and organisational measures to safeguard the security of any electronic communications networks or services provided to Controller or utilised to transfer or transmit Controller data.

(2) This includes but is not limited to measures designed to ensure the secrecy of communications and prevent unlawful surveillance or interception of communications and gaining unauthorised access to any computer or system and thus guaranteeing the security of the communications.

8. Privacy Impact Assessment

The Processor shall make available to the Controller – at its request - all information necessary to demonstrate Controller's compliance with the Applicable Law and shall assist Controller to carry out a privacy impact assessment of the Services and work with Controller to implement agreed mitigation actions to address privacy risks so identified.

9. Right to Audit

(1) Controller has the right to carry out inspections or to have them carried out by an auditor (each an "Auditing Party) to be designated in each individual case. Controller has the right to convince itself of the compliance with this agreement by the Processor in his business operations by means of random checks, upon due prior notification.

(2) The Processor shall ensure that Controller is able to verify compliance with the obligations of Processor in accordance with Article 28 GDPR. The Processor undertakes to give Controller the

necessary information on request and, in particular, to demonstrate the execution of the technical and organizational measures.

(3) Evidence of such measures, which concern not only the specific Service, may be provided by

a. Compliance with approved Codes of Conduct pursuant to Article 40 GDPR;

b. Certification according to an approved certification procedure in accordance with Article 42 GDPR;

c. Current auditor's certificates, reports or excerpts from reports provided by independent bodies (e.g. auditor, Data Protection Officer, IT security department, data privacy auditor, quality auditor)

d. A suitable certification by IT security or data protection auditing (e.g. ISO/IEC 27001).

(4) The Auditing Party shall bear its own costs in relation to such audit, unless the audit reveals any non-compliance with Processor's or Subprocessor's obligations under any Applicable Law or this Agreement, in which case the costs of the audit shall be borne by the Processor.

(5) Processor shall remedy any deficits found within a reasonable period at its own expense, failing which controller may terminate the Agreement prematurely for good cause.

10. Deletion of Personal Data

(1) The Processor shall delete Personal Data from the Service(s) in accordance with the retention policies set out in the relevant Processing Appendix for the Service(s) and at such other times as may be required from time to time by Controller.

(2) At any time during the term of this Agreement or upon its (or its Services') termination or expiry, any remaining Personal Data shall, at Controller's option, be destroyed or returned to Controller, along with any medium or document containing Personal Data.

11. Third Party Requests for Disclosure

(1) Unless prohibited by Applicable Law, the Processor shall, and shall procure that the Subprocessor shall, inform Controller promptly of any inquiry, communication, request, claim or complaint from:

a. any governmental, regulatory or supervisory authority, including Privacy Authorities; and/or

b. any court of law (legal request);

c. any data subject;

(2) In such case, the Processor shall provide all reasonable assistance to Controller without additional cost to enable Controller to respond to such inquiries, communications, requests or complaints and to meet applicable statutory or regulatory deadlines.

(3) The Processor shall, and it shall procure that any Subprocessor shall, not disclose Personal Data to any of the persons or entities above unless it is legally prohibited from doing.

12. Indemnity

Notwithstanding any other indemnity provided by the Processor in connection with the Processing subject to the Framework Agreement, the Processor shall indemnify Controller (and each of their respective officers, employees and agents) against all losses (including any claim, damage, cost, charge, fine, fees, levies, award, expense or other liability of any nature, whether direct, indirect, or consequential) arising out of or in connection with any failure by the Processor (and by any Subprocessor) to comply with the provisions of this Agreement or any Applicable Law.

13. Term and Termination

(1) This contract shall continue in full force and effect until the later of (i) the termination or expiration of the Agreement; or (ii) the termination of the last of the services to be performed pursuant to the Agreement.

(2) The provisions of this Agreement shall apply to any Processing of Personal Data received prior to execution during any transitional or migration phase.

14. Governing Law

This Agreement shall be exclusively subject to Austrian law - in particular, the Austrian data protection law, including GDPR, as well as any guidelines or codes of conduct issued by the Privacy Authority - excluding its conflict of laws principles and the UN Sales Convention. Moreover, the competent court shall be the relevant court for A-1010 Vienna which has the subject-matter jurisdiction.

Schedule 1 - Standard Contractual Clauses

It is hereby stated that the Standard Contractual Clauses do not apply in the direct relationship between the parties. In the case of subcontracting pursuant point 6. the Standard Contractual Clauses may apply between the Processor and a Subprocessor.

Schedule 2 - Processing Appendix

1. Nature and Purpose of the intended Processing of Data

The Nature and Purpose of Processing of Personal Data by Processor for Controller are defined in the Agreement.

The undertaking of the contractually agreed Processing of Data shall be carried out exclusively within a Member State of the European Union (EU) or within a Member State of the European Economic Area (EEA). Each and every Transfer of Data to a State which is not a Member State of either the EU or the EEA requires the prior agreement of the Client and shall only occur if the specific Conditions of Article 44 et seq. GDPR have been fulfilled.

2. Type of Data

The subject matter of the Processing of Personal Data may comprise of the following data types/categories based on the Agreement:

(1) Person master data (e.g. name, address)
(2) Person identification
(3) Special categories of personal data (e.g. political orientation, religion, biometric data)
(4) Personalized marketing and sales data (e.g. target group, turnover)
(5) Personal roles and associations (e.g. administrator, user, recipient of invoice)
(6) Customer inventory (e.g. customer product, customer number, contract number)
(7) Customer interaction (e.g. offer, order, contract termination)
(8) Documents (e.g. contracts, declaration of consent, copy passport)
(9) Traffic data (e.g. time of call, number called, IP address, TAP files)
(10) Geolocation data (e.g. cell ID, GPS data)
(11) Content data (e.g. browsing logs, chat, email, voicemail)
(12) Financial data (e.g. bank account data, payment conditions)
(13) Employee-Login data (e.g. corporate account, employee email address, sales ID, User ID)

3. Categories of Data Subjects

The Categories of Data Subjects affected by the processing may include the following:

(1) Contract partner Customer natural person
(2) Contract partner Customer legal person
(3) Contract partner Employee of Customer
(4) Authorized User of Enterprise Customer
(5) Children
(6) Vulnerable natural persons (handicapped, ill)
(7) Prospects
(8) Controller’s employees
(9) Controller’s suppliers, business partners, agents
(10) Controller’s contact persons of suppliers, business partners, agents

(11) Other contact person of the Controller

4. General description of the technical and organisational security measures referred to in Article 32(1) of the GDPR

Before the commencement of processing, the Processor shall document the execution of the necessary Technical and Organisational Measures set out in advance of the awarding of the contract, specifically with regard to the detailed execution of the contract, and shall present these documented measures to Controller for evaluation.

Upon acceptance by Controller, the documented measures become integral part of the contract. Insofar as the inspection/audit performed by Controller reveals the need for amendments, such amendments shall be implemented by mutual agreement.