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

Company of Telekom Austria Group (TAG) hereinafter referred to as „Controller"	and	Contractual Partner hereinafter referred to as "Processor"

agree:

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 as defined in this AGREEMENT it may be necessary for the processor to process certain data on behalf of CONTROLLER.

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

General Data Protection Regulation (GDPR)	shall mean the Regulation (EU) 2016/679 on the protection of natural persons with regard to the PROCESSING of PERSONAL DATA which has been in force since May 25, 2018 in the applicable version;
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 (Annex 1) 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 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.

2.2 Information Security

PROCESSOR shall keep PERSONAL DATA logically separate to data PROCESSED on behalf of any other third party.

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.

PROCESSOR assures to comply with the Security Requirements ofCONTROLLER. These Security Requirements are available for viewing, printing and downloading:

https://www.a1.net/lieferanteninformation-eng → Miscellaneous → Information Security Requirements.
These security requirements are determined in the "A1 Information Security Standard for secure service operation". Unless otherwise agreed, the PROCESSOR shall comply with those security requirements which are specified in the "Extended Protection" protection needs.

CONTROLLER may unilaterally amend these 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.

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 CONTROLLERunder this contract or otherwise, CONTROLLER shall have the option to:

- 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

- restore itself or procure the restoration of the PERSONAL DATA and require the PROCESSOR to reimburse CONTROLLERfor any reasonable costs incurred in so doing.

2.3 PROCESSING of PERSONAL DATA

The PROCESSOR warrants in respect of all PERSONAL DATA that it PROCESSES on behalf of CONTROLLER, that:

a. PROCESSOR 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. PROCESSOR shall not itself exercise control, nor shall transfer PERSONAL DATA to a third party, unless expressly specified otherwise by CONTROLLER;

c. PROCESSOR shall not PROCESS, apply or use the PERSONAL DATA for any purpose other than as required and is necessary to provide the services;

d. PROCESSOR shall not PROCESS PERSONAL DATA for its own purposes or include PERSONAL DATA in any product or service offered to third parties.

In order to ensure that CONTROLLER's's instructions in respect of any PERSONAL DATA can be carried out as required under this contract, the PROCESSOR shall have in place appropriate processes and any associated technical measures, including the following:

e. The duty to assist CONTROLLERwith 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;

f. updating, amending or correcting the PERSONAL DATA of any data subject upon request of CONTROLLER from time to time;

g. cancelling or blocking access to any PERSONAL DATA upon receipt of instructions from CONTROLLER;

h. 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.

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.

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.

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.

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.

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

3 Data Breach and Notification Requirements

PROCESSOR shall immediately, but not later than 20 hours, inform CONTROLLER after becoming aware of any accidental, unauthorized, or unlawful (a) destruction, (b) loss, (c) alteration, or d) disclosure of, or e) access to, PERSONAL DATA ("SECURITY BREACH").

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.

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.

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.

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.

In the event the SECURITY BREACH will impact more CONTROLLER's customers, PROCESSOR shall prioritize CONTROLLER in providing support and implement necessary actions and remedies.

4 PROCESSOR Employees – Confidentiality

PROCESSOR shall ensure the reliability of any employees and subcontractors 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 AGREEMENT.

Processor will remain liable for any disclosure of PERSONAL DATA by each such person as if it had made such disclosure.

5 Subprocessing

For the purposes of this clause, subcontracting shall mean services which are directly related to the provision of the services referred to in Annex 1.

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.

PROCESSOR is not allowed to sub-contract or outsource any PROCESSING of PERSONAL DATA to any other person or entity, including its affiliated companies unless and until (cumulatively):

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 and

    ii. details (including categories) of the PROCESSING to be carried out by the subprocessor in relation to the services referred to in Annex 1;

    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 and

b. PROCESSOR has made legally binding contractual agreements no less onerous than those contained in this contract on such subprocessor.

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 (and the persons who, through the subprocessor, have access to or influence on the PERSONAL DATA of CONTROLLER) as if they were the acts or omissions of the PROCESSOR.

6 Security of Communications

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's data.

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.

7 Right to Audit

CONTROLLER has the right to carry out inspections or to have them carried out by an auditor 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.

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.

Evidence of such measures, which concern not only the specific service, may be provided by

i. Compliance with approved Codes of Conduct pursuant to Article 40 GDPR;
ii. Certification according to an approved certification procedure in accordance with Article 42 GDPR;
iii. 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)

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

The costs for the audit are borne by CONTROLLER; 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. 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.

8 Deletion of Personal Data

Upon CONTROLLER's request, at any time during the term of this contract or upon its termination, the PROCESSOR shall either destroy or return to CONTROLLER (together with any media or documents containing such media) any PERSONAL DATA remaining with the PROCESSOR.

PROCESSOR shall follow CONTROLLER's instructions to return or delete the PERSONAL DATA.

9 Third Party Requests for Disclosure

Unless prohibited by applicable law, the PROCESSOR shall inform CONTROLLER promptly of any inquiry, communication, request, claim or complaint from any governmental, regulatory or supervisory authority, (including PRIVACY AUTHORITY), any court of law (legal request) or any data subject regarding PERSONAL DATA.

In such case, 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.

PROCESSOR shall not disclose any PERSONAL DATA to third parties unless the PROCESSOR is required to do so by law. The PROCESSOR shall also ensure that this obligation is fulfilled by all its subprocessors.

10 Indemnity

Notwithstanding any other indemnity provided by the Processor in connection with the PROCESSING subject to the 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 contract or any applicable law.

Any contractual penalties agreed in the AGREEMENT shall remain unchanged.

11 Term and Termination

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.

The provisions of this contract shall apply to any PROCESSING of PERSONAL DATA received prior to execution during any transitional or migration phase.

12 Governing Law

This contract 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.

Annex 1 – Processing of personal data by the processor

a. Nature and purpose of the provided processing

The nature and purpose of the processing of personal data by the processor for CONTROLLER are defined in the Framework Agreement.

b. Nature of the personal data

The data (of the following types) that the processor processes based on the Service Agreement includes the following:

- Personal master data
- Personal identifiers
- Special categories of personal data & biometric data
- Marketing/sales data with personal reference
- Personal role & associations
- Customer inventory
- Customer interaction
- Documents
- Traffic data
- Geolocation data
- Content data
- Financial data
- Employee login

c. Categories of affected persons

The groups affected by the processing include the following:

- Contract partner Customer natural person
- Contract partner Customer legal person
- Contract partner Employee of Customer
- Authorized User
- of Enterprise Customer
- Children
- Vulnerable natural persons (handicapped, ill)
- Prospects
- CONTROLLER's employees
- CONTROLLER's suppliers and sales partners
- CONTROLLER's contact persons for suppliers and sales partner

d. General description of the Technical and Organisational measures pursuant to article 32 (1) GDPR

Before starting the processing, the processor will document the implementation of the required technical and organisational measures and submit for control to CONTROLLER. Except in the event of reasonable refusal by CONTROLLER, the documented measures will form the base for the processing of the personal data provided by CONTROLLER regarding the Service Agreement.