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shall mean the Regulation (EU) 2016/679 coming into effect on May 25, 2018 according to which the Directive 95/46/EC is repealed;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 organizational security measures to protect Personal Data against accidental, unlawful destruction or accidental loss, damage, alteration, unauthorized 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 endeavors 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 , Module 2, "Transfer controller to processor" (Schedule 1), 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 organizational measures to safeguard the security of any electronic communications networks or services provided to Controller or utilized 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 unauthorized 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

Controller to Processor
(Module 2)

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data

subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organizational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymization, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymization, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organizational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defense of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) OPTION 1: SPECIFIC PRIOR AUTHORISATION The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorization. The data importer shall submit the request for specific authorization at least 180 days prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorization. The list of sub-processors already authorized by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorized to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organizational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller,

to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a

democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules.

These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Austria.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Austria.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Controller of the DPA

Contact person's name, position and contact details:
Framework Agreement

Activities relevant to the data transferred under these Clauses:
Schedule 2 of the DPA, Framework Agreement

Role (controller/processor):
Controller

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name/ Address:
Contractor/Processor of the DPA

Contact person's name, position and contact details:
Schedule 4 of the DPA

Activities relevant to the data transferred under these Clauses:
Schedule 2 of the DPA

Role (controller/processor):
Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred
Schedule 2 of the DPA

Categories of personal data transferred
Schedule 2 of the DPA

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.
Schedule 2 of the DPA, A1 Digital Information Security Requirements for Suppliers

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Data is transferred on a continuous basis.

Nature of the processing
Schedule 2 of the DPA, Framework Agreement

Purpose(s) of the data transfer and further processing
Framework Agreement

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Framework Agreement

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing
Framework Agreement

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

Framework Agreement

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Chapter 2.2 ***Error! Reference source not found.*** *of the DPA*

For transfers to (sub-) processors, also describe the specific technical and organizational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

Schedule 2, Framework Agreement

ANNEX III

LIST OF SUB-PROCESSORS

The controller has authorized the use of the following sub-processors:

1. Name: …

   Address: …

   Contact person's name, position and contact details: …

   Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorized): …

2. …

Framework Agreement

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 organizational 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 Organizational Measures set out in advance of the awarding of the contract, specifically regarding 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.