DATA PROCESSOR AGREEMENT (DPA)

This data processing agreement forms part of the 'WhatConverts Terms of Use' ("Principal Contract") available here https://www.whatconverts.com/terms and is made effective from _____ between the undersigned parties:

Icon Digital LLC (DBA WhatConverts) **(*"Processor"*)** By:_____ Name:_____ Title:_____ Signature Date:_____ Address: 1409 Coachman Drive Waxhaw, NC 28173 United States of America	**Customer Name (Required)** **("*Controller*")** (Full legal entity Name) By:_____ Name:_____ Title:_____ Signature Date:_____ Customer Address: (**Required**): _____ _____ _____

Instructions

This Agreement has been pre-signed on behalf of Icon Digital (DBA WhatConverts). To enter into this Agreement, Customer must:

● Complete the table above by signing and providing the customer full legal entity name, address and signatory information; and Complete the data exporting organisation found on page 6, 11 and 13.

● Submit the completed and signed Addendum to WhatConverts via email to support@whatconverts.com.

● Customer signatory represents to Icon Digital, LLC that he or she has the legal authority to bind the Customer.

● This Addendum will terminate automatically upon termination of the Principal Contract.

1. Terms of Agreement

1.1. This agreement supplements the Principal Contract and makes legally binding provisions for compliance with the Data Protection Laws as set forth in this agreement. As per the requirements of relevant Data Protection Law, all processing of personal data by a processor on behalf of a controller, shall be governed by a contract. The terms, obligations and rights set forth in this agreement relate directly to the data processing activities and conditions laid out in Schedule 1.

1.2. The terms used in this agreement have the meanings as set out in the 'definitions' part of the document.

2. Definitions

2.1. In this Agreement, unless the text specifically notes otherwise, the below words shall have the following meanings: -

2.2. "Consent" of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

2.3. "Data Protection Laws" means all applicable Data Protection Laws, including the General Data Protection Regulation (GDPR) (EU 2016/679), [Data Protection Bill] and, to the extent applicable, the data protection or privacy laws of any other country.

2.4. "EEA" means the European Economic Area.

2.5. "Effective Date" means the date that this agreement comes into force.

2.6. "Personal Data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

2.7. "GDPR" means the General Data Protection Regulation (GDPR) (EU) (2016/679)

2.8. "Principal Contract" means the WhatConverts Terms of Service.

2.9. "Processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

2.10. "Recipient" means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

2.11. "Third-party" means a natural or legal person, public authority, agency or body other than the data subject, Controller, Processor and persons who, under the direct authority of the Controller or Processor, are authorised to process personal data.

2.12. "Sub Processor" means any person or entity appointed by or on behalf of the Processor to process personal data on behalf of the Controller"Supervisory authority" means an independent public authority which is established by a Member State pursuant to Article 51 of the "GDPR".

3. Obligations and Rights of the Processor

3.1. The Processor shall comply with the relevant Data Protection Laws and as well as the following:

A. only act on the documented instructions of the Controller, unless required by EU or Member State law to which the Processor is subject, in which case, the Processor shall to the extent permitted by such law inform the Controller of that legal requirement before the relevant Processing of that Personal Data;

B. Assist the Data Controller in ensuring compliance with obligations regarding security of processing, notifications of personal data breaches to the corresponding supervisory authority and to the affected data subjects, data protection impact assessment and prior consultations pursuant to articles 32 to 36 GDPR or applicable local data protection regulation, taking into account the nature of processing and the information available to the Data Processor.

C. Ensure that each of its employees, agents, subcontractors or vendors authorized to process personal data are bound by a duty of confidentiality and are made aware of its obligations regarding the security and protection of the personal data and the terms set out in this agreement.

D. Implement the technical and organizational security measures in accordance with article 32 GDPR, for which purposes the Data Processor undertakes to assess potential risks arising from the data processing activities that it carries out, taking into account the means that are used to provide the services (technology, resources, etc.) and other circumstances which may have a security impact.

E. Promptly notify the Controller if it receives any communication from a Data Subject or Supervisory Authority under any Data Protection Laws in respect of the Personal Data, including requests by a Data Subject to exercise rights in Chapter III of GDPR and assist the Controller in the Controller's obligation to respond to these communications. Processor shall be given reasonable time to assist the Controller with such requests in accordance with the Applicable Law.

F. Following expiration or termination of the Agreement, the Processor will delete or return to the Controller all Personal Data in its possession as provided in the Agreement (or, if sooner, the service to which it relates) except to the extent the Processor is required by Applicable law to retain some or all of the personal data (in which case the Processor will implement reasonable measures to prevent the personal data from any further processing). The terms of this DPA will continue to apply to such Personal Data.

G. make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in the relevant Data Protection Laws and allow for, and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller.

H. inform the the Controller without undue delay if the instructions received are infringing the GDPR or other Data Protection Law of the EU or a member state.

I. In the event that the Processor becomes aware of any personal data breach involving data that the Controller has disclosed to the Processor, the Processor shall notify the Controller without undue delay after becoming aware of the said personal data breach. Taking into account the nature of the processing and the information available to the Processor, the Processor shall assist the

Controller in ensuring compliance with the Controller's personal data breach notification obligations to the supervisory authority and data subjects under Data Protection Law;
J. where applicable, employ a Data Protection Officer if required.
K. where applicable, appoint a representative within the EU if required in accordance with GDPR Article 27.

3.2. Nothing within this agreement relieves the processor of their own direct responsibilities, obligations and liabilities under the General Data Protection Regulation (GDPR) or other Data Protection Laws.

3.3 The parties acknowledge that in providing the services under this Agreement, the Processor may transfer Personal Data to a sub-processor (as importer) located in a Third Country ("International Transfers"). The Customer consents to such International Transfer, where either (i) the data recipient or the country in which it operates has been determined by the European Commission to ensure an adequate level of protection for the rights and freedoms of Data Subjects in relation to their Personal Data; (ii) WhatConverts' has entered into Standard Contractual Clauses (Processors) (as laid down in the Implementing Decision 914/2021/EU on standard contractual clauses for the transfer of personal data to third countries pursuant Regulation (EU) 679/2016) ("Standard Contractual Clauses"), under which the Customer (as exporter) will have direct contractual rights of enforcement against the sub-processor (as importer) – Schedule 3; (iii) the Processor has ensured another appropriate data transfer safeguard is in place in compliance with Chapter V of the GDPR.

3.4 Outsourcing
3.4.1 The Data Controller grants general authorization to Data Processor to engage other data processors for the processing of the Personal Data. Moreover, it also grants general authorization in order for such sub-data processors to also subcontract to other sub-data processors.

3.4.2 The Sub-data processor(s) currently engaged in the processing of Personal Data are included in Appendix II. When the Data Processor engages other companies, the Data Processor shall inform the Data Controller of any intended changes at least 30 days in advance, being deemed automatically included in such Appendix as of such notification, without the need of updating such Appendix.

3.4.3 When the Data Processor engages another Data Processor for carrying out specific processing activities on behalf of the Data Controller, the Data Processor is obliged to sign a Sub-data processing agreement subject to the terms foreseen in this DPA.

3.4.4 The sub-data processor is considered as a data processor and shall not process Personal Data except on instructions from the Data Controller and the Clauses of this DPA. The Data Processor should regulate the new contractual relationship so that the same data protection obligations (instructions, security measures, duties, etc.) and the same formal requirements regarding data processing and rights and freedoms of data subjects are fulfilled by the sub-data processor.

3.6. The Processor shall maintain a record of all categories of processing activities carried out on behalf of the Controller, containing: -

- the name and contact details of the Processor
- the categories of processing carried out on behalf of each Controller
- transfers of personal data to a third country or an international organisation, including the identification of

that third country or international organisation and, the documentation of suitable safeguards

- a general description of the technical and organisational security measures referred to in Article 32(1)

3.7. The Processor shall maintain records of processing activities in writing and electronic form and shall make the record available to the supervisory authority on request

3.8. When assessing the appropriate level of security and the subsequent technical and operational measures, the Processor shall consider the risks presented by any processing activities, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

4. Controller obligations

4.1 The Customer represents, undertakes and warrants that all personal data processed by WhatConverts has been and shall be collected and processed by the Customer in accordance with Data Protection Laws and without limitation to the foregoing, the Customer shall take all steps necessary, including without limitation providing appropriate fair collection notices and ensuring that there is a lawful basis for Customer to process the personal data, to ensure that the processing of the personal data by WhatConverts in accordance with this Agreement is in accordance with Data Protection Laws.

5. Relationship with the Principal Contract

5.1. Except for the changes made by this DPA, the principal contract remains unchanged and in full force and effect. If there is any conflict between this DPA and the principal agreement, this DPA shall prevail to the extent of that conflict.

5.2. Any claims brought under or in connection with this DPA shall be subject to the terms of Use, including but not limited to, the exclusions and limitations set forth in the principal contract.

6. General Information

6.1. This DPA applies where and only to the extent that The Processor processes personal data that originates from the EEA and/or that is otherwise subject to EU Data Protection Law on behalf of Customer as Data Processor in the course of providing services pursuant to the principal contract.
6.2. The Controller agrees that (i) it shall comply with its obligations as a Data Controller under Data Protection Laws in respect of its processing of personal data and any processing instructions it issues to The Processor; and (ii) it has provided notice and obtained (or shall obtain) all consents and rights necessary under Data Protection Laws for The Processor to process Customer Data and provide the services pursuant to the principal contract and this DPA.
6.3. Both parties assume their responsibilities respectively for the use of personal data in accordance with the GDPR and all applicable data protection laws with regard to the obligations of the Controller and the Processor.
6.4. In fulfillment of its obligations The Processor will only be liable in case of breaking the commands expressed by the Controller.
6.5. No one other than a party to this DPA, its successors and permitted assignees shall have any right to enforce any of its terms.

Appendix I - Processing Details

a. The Controller named in this agreement has appointed The Processor with regard to specific processing activity requirements. These requirements relate to provision of The Processor's platform and services.
b. The duration of the data processing under this DPA is until the termination of the principal contract in accordance with its terms.
c. The purpose of the data processing under this DPA is the provision of the 'WhatConverts' Services and the performance of The Processor's obligations under the principal contract and this DPA or as otherwise agreed by the parties.
d. The requirement for the named Processor to act on behalf of the Controller is with regard to the below type(s) of personal data and categories of data subjects: -

- Controller and User data including: identification and contact data (name, date of birth, gender, general, occupation or other demographic information, address, title, contact details, including email address), personal interests or preferences (including purchase history, marketing preferences and publicly available social media profile information); IT information (IP addresses, usage data, cookies data, online navigation data, location data, browser data); financial information (credit card details, account details, payment information).
- Any individual accessing and/or using the 'WhatConverts' platform through the Customer's account ("Users") and whose information is stored on or collected via the 'WhatConverts' platform.

Appendix II - Authorized Sub Processors List

Sub Processor Name	Contact Details	Purpose of Processing	Type of Data Processed
Amazon Web Services	https://aws.amazon.com	Data Storage and Processing	User and Marketing Data
Twilio	https://www.twilio.com	Call Routing	Caller Data
Bandwidth	https://www.bandwidth.com	Call Routing	Caller Data
AssemblyAI	https://www.assemblyai.com	Call Transcription	Call Contents

Appendix III - Standard Contractual Clauses

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)[1] for the transfer of personal 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

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision […].

(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 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(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

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 organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised 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 pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, 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 organisational 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 authorised 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[2] (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 defence 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

---

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

(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) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(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.[3] 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

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

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 authorised 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 organisational 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 of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, 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[4];

(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.

---

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

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.). [For Module Three: The data exporter shall forward the information to the controller.]

(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 [for Module Three: and the controller] 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 the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of the Member State of the exporter's "EU representative" under Article 27 GDPR.

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.

(f) The Parties agree that those shall be the courts of of the exporter's "EU representative" under Article 27 GDPR.

(g) 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.

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

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

The relevant details for this section are to be found in the Principal Agreement, in Appendix I of the above "Data Processing Agreement" and/or the respective purchasing order, statement of work, and agreement.

Role controller

Data importer:

The relevant details for this section are to be found in the Principal Agreement, in Appendix I of the above "Data Processing Agreement" and/or the respective purchasing order, statement of work, and agreement.

Role processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

The relevant details for this section are to be found in the Principal Agreement, in Appendix I of the above "Data Processing Agreement" and/or the respective purchasing order, statement of work and agreement.

Categories of personal data transferred

The relevant details for this section are to be found in the Principal Agreement, in Appendix I of the above "Data Processing Agreement" and/or the respective purchasing order, statement of work, and agreement.

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 specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

The relevant details for this section are to be found in the Principal Agreement, in Appendix I of the above "Data Processing Agreement" and/or the respective purchasing order, statement of work, and agreement.

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

The relevant details for this section are to be found in the Principal Agreement, in Appendix I of the above "Data Processing Agreement" and/or the respective purchasing order, statement of work, and agreement.

Nature of the processing

Receiving Personal Data, accessing, storing, retrieving, combining, analyzing, modifying, anonymizing and recording the same; any other Processing operation as deemed necessary to perform the Services under the Principle Agreement and/or the respective purchasing order, statement of work and agreement.

Purpose(s) of the data transfer and further processing

For purposes strictly necessary for the performance of the Services under the Principle Agreement and/or the respective purchasing order, statement of work and agreement.

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

For the duration strictly necessary for the performance of the Services under the Agreement and/or the respective purchasing order, statement of work and agreement and following termination or expiration of the Principal Agreement, for such duration as otherwise permitted or required by law.

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

Subject matter, nature and duration for the sub processors referred to in Appendix II - Authorized sub processors list can be found in the relevant data protection clauses in the commercial contracts.

C. COMPETENT SUPERVISORY AUTHORITY

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

The Parties agree that this shall be the supervisory authority of the Member State of the exporter's "EU representative" under Article 27 GDPR.

ANNEX II

Technical And Organisational Measures Including Technical And Organisational Measures To Ensure The Security Of The Data

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Processor utilises third-party data centers that maintain current ISO 27001 certifications and/or SSAE 16 SOC 1 Type II or SOC 2 Attestation Reports. The Processor will not utilise third party data centers that do not maintain the aforementioned certifications and/or attestations, or other substantially similar or equivalent certifications and/or attestations.

Upon the Controller's written request (no more than once in any 12 month period), the Processor shall provide within a reasonable time, a copy of the most recently completed certification and/or attestation reports (to the extent that to do so does not prejudice the overall security of the Software and Services). Any audit report submitted to the Controller shall be treated as Confidential Information and subject to the confidentiality provisions of the Agreement between the parties.

The following descriptions provide an overview of the technical and organisational security measures implemented.

It should be noted however that, in some circumstances, in order to protect the integrity of the security measures and in the context of data security, detailed descriptions may not be available, however additional information regarding technical and organisational measures may be found in the Security Policy. It's acknowledged and agreed that the Security Policy and the technical and organisational measures described therein will be updated and amended from time to time, at the sole discretion of the Processor. Notwithstanding the foregoing, the technical and organisational measures will not fall short of those measures described in the Security Policy in any material, detrimental way.

Entrance Control

Technical or organisational measures regarding access control, especially regarding legitimation of authorised persons: The aim of the entrance control is to prevent unauthorised people from physically accessing such data processing equipment which processes or uses Personal Data. Due to their respective security requirements, business premises and facilities are subdivided into different security zones with different access authorisations. Access to the data center is monitored by security personnel. Access for employees is only possible with an encoded ID with a photo on it. All other persons have access only after having registered before (e.g. at the main entrance). Access to special security areas for remote maintenance is additionally protected by a separate access area. The constructional and substantive security standards comply with the security requirements for data centers.

System Access Control

Technical and organisational measures regarding the user ID and authentication: The aim of the system access control is to prevent unauthorised use of data processing systems, are used for the

processing of Customer Data. Authorisation is executed by providing a unique username and password to a centralised directory service. All access attempts, successful and unsuccessful are logged and monitored. Additional technical protections are in place using firewalls and proxy servers and state of the art encryption technology that is applied where appropriate to meet the protective purpose based on risk.

Data Access Control

Technical and organisational measures regarding the on-demand structure of the authorisation concept, data access rights and monitoring and recording of the same: Access to data necessary for the performance of the particular task is ensured within the systems and applications by a corresponding role and authorisation concept. In accordance to the "least privilege" and "need-to-know" principles, each role has only those rights which are necessary for the fulfilment of the task to be performed by the individual person. To maintain data access control, state of the art encryption technology is applied to the Personal Data itself where deemed appropriate to protect sensitive data based on risk.

Transmission Control

Technical and organisational measures regarding the transport, transfer, transmission, storage and subsequent review of Personal Data on data media (manually or electronically). Transmission control is implemented so that Personal Data cannot be read, copied, changed or deleted without authorisation, during transfer or while stored on data media, and so that it can be monitored and determined as to which recipients a transfer of Personal Data is intended. The measures necessary to ensure data security during transport, transfer and transmission of Personal Data as well as any other company or Customer Data are detailed in the Security Policy. This standard includes a description of the protection required during the processing of data, from the creation of such data to deletion, including the protection of such data in accordance with the data classification level. For the purpose of transfer control, an encryption technology is used (e.g. remote access to the company network via two factor VPN tunnel and full disk encryption). The suitability of an encryption technology is measured against the protective purpose. The transfer of Personal Data to a third party (e.g. customers, sub-contractors, service providers) is only made if a corresponding contract exists, and only for the specific purposes. If Personal Data is transferred to companies located outside the EEA, the Processor provides that an adequate level of data protection exists at the target location or organisation in accordance with the European Union's data protection requirements, e.g. by employing contracts based on the Standard Contractual Clauses.

Data Entry Control

Technical and organisational measures regarding recording and monitoring of the circumstances of data entry to enable retroactive review. System inputs are recorded in the form of log files therefore it is possible to review retroactively whether and by whom Personal Data was entered, altered or deleted.

Data Processing Control

Technical and organisational measures to differentiate between the competences of principal and contractor: The aim of the data processing control is to provide that Personal Data is processed by a commissioned data processor in accordance with the Instructions of the principal. Details regarding data processing control are set forth in the Agreement and DPA.

Availability Control

Technical and organisational measures regarding data backup (physical/logical): Data is stored across multiple centres in geographically different locations. The data centres can be switched in the event of flooding, earthquake, fire or other physical destruction or power outage protecting Personal Data against accidental destruction and loss. If Personal Data is no longer required for the purposes for which it was processed, it is deleted promptly. It should be noted that with each deletion, the Personal Data is only locked in the first instance and is then deleted for good with a certain delay. This is done in order to prevent accidental deletions or possible intentional damage.

Separation Control

Technical and organisational measures regarding purposes of collection and separated processing:

Personal Data used for internal purposes only e.g. as part of the respective customer relationship, may be transferred to a third party such as a subcontractor, solely under consideration of contractual arrangements and appropriate data protection regulatory requirements.

Employees are instructed to collect, process and use Personal Data only within the framework and for the purposes of their duties (e.g. service provision). At a technical level, multi-client capability includes separation of functions as well as appropriate separation of testing and production systems.

Customer Data is stored in a way that logically separates it from other customer data.

The Controller is assigned a unique encryption key, generated using a FIPS 140-2 compliant crypto library, which is used to encrypt and decrypt all of the Controller's archived data. In addition to the unique encryption keys, all data being written to the storage grid includes the Controller's unique account code. The Processor's systems that write data to the storage grid retrieve the encryption key from one system and the customer code from another, which serves as a cross check against two independent systems. The Controller's encryption key is further encrypted with

a Processor key stored within a centralised and restricted key management system. In order for the Processor to access Customer Data via the master key, the key management system provisions individual keys following a strict process of approval that includes multiple levels of executive authorisation. Use of these master encryption keys is limited to senior production engineers and all access is logged, monitored, and configured for alerting by security via a centralised Security Incident and Event Management ("SIEM") system. The Controller's archived data is encrypted at rest using AES256 bit encryption and data in transit is protected by Transport Layer Security ("TLS").