Fuse Data Processing Addendum

Last updated: 9 August 2024

1. Data Processing Agreement preamble

1.1. This Data Processing Agreement ("**DPA**") is entered into between Fuse Universal Ltd ("**Data Processor**") and the Customer ("**Data Controller**") (together the "**Parties**") and sets out the rights and obligations that apply to the Data Processor's handling of Personal Data on behalf of the Data Controller. **"Personal Data**" shall mean personal data as defined by the Applicable Data Protection Laws.

1.2. This DPA is incorporated by reference into the Master Customer Agreement dated between the Parties ("**Agreement**") for the supply of Services by the Data Processor to the Data Controller.

1.3. This DPA has been designed to ensure the Parties' compliance with Applicable Data Protection Laws. "**Applicable Data Protection Laws**" shall mean all applicable federal, state and foreign data protection, privacy and data security laws, regulations, and directives, including, without limitation, the General Data Protection Regulation (Regulation (EU) 2016/679) ("**EU GDPR**"), the UK Data Protection Act 2018 ("**UK GDPR**") and the California Consumer Privacy Act of 2018 ("**CCPA**").

1.4. The terms used in this DPA shall have the meanings set forth in this DPA. Capitalised terms not otherwise defined herein shall have the meaning given to them in the Agreement. Except as modified below, the terms of the Agreement shall remain in full force and effect.

1.5. This DPA shall not exempt the Parties from their respective obligations under Applicable Data Protection Laws.

Now therefore, in consideration of the mutual promises herein and other good and valuable consideration, the Parties to this DPA agree as follows:

2. The rights and obligations of the Data Controller and processing of Personal Data

2.1. The Data Controller appoints the Data Processor to process the Personal Data described in Appendix A.

2.2. The details on the subject matter, duration, nature and purpose of processing and the Personal Data categories and data subject types in respect of which will be subjected to processing by the Data Processor in the performance of the Services pursuant to the Agreement are specified in Appendix A.

2.3. The Data Controller shall have both the right and obligation to make decisions about the purposes and means of the processing of Personal Data and shall be responsible for ensuring that the processing that the Data Processor is instructed to perform is authorised by law.

3. Obligations of the Data Processor

3.1. The Data Processor shall solely be permitted to process Personal Data on documented instructions from the Data Controller to the extent necessary to perform its obligations under the Agreement, unless processing is required under UK, EU or Member State law to which the Data Processor is subject. In this case, and where possible to do so, the Data Processor shall inform the Data Controller of this legal requirement prior to processing unless that law prohibits disclosure of such information on important grounds of public interest.

3.2. The Data Processor shall inform the Data Controller as soon as reasonably possible if the instructions, in the opinion of the Data Processor, contravene the Applicable Data Protection Laws .

4. Confidentiality

4.1. The Data Processor shall reasonably ensure that:

a) only those persons who are currently authorised to do so are able to access the Personal Data being processed on behalf of the Data Controller;
b) only persons who require access to the Personal Data in order to fulfil the obligations of the Data Processor to the Data Controller shall be provided with authorisation; and
c) that persons authorised to process Personal Data on behalf of the Data Controller have undertaken to observe confidentiality or are subject to a duty of confidentiality which offers a degree of protection which is at least equivalent to that offered under the Agreement.

5. Security of processing

5.1. The Data Processor shall implement appropriate technical and organisational measures to protect the Personal Data (i) from accidental or unlawful destruction, and (ii) loss, alteration, unauthorised disclosure of, or access to the Personal Data ("**Safeguards**").
5.2. Safeguards shall, taking into account the state of the art and the costs of the implementation and execution of the measures, ensure an adequate level of protection taking into account the risks involved in the processing and the nature of the Personal Data to be secured.
5.3. The Data Processor shall, in ensuring the above – in all cases –implement the level of security and the measures specified in Appendix C to this DPA.
5.4. Where the Parties agree on the requirement of establishing additional security measures, the terms and cost of implementing such measures shall be dealt with in the Agreement.

6. Use of Sub-Processors

6.1. The Data Processor shall not engage a third-party processor ("**Sub-Processor**") for the fulfilment of this DPA without the prior consent of the Data Controller.
6.2. A list of approved Sub-Processors as at the date of this DPA is listed in Appendix B to this DPA and the Data Processor shall maintain and provide updated copies of this list to the Data Controller when it adds or removes Sub-Processors in accordance with this Agreement.
6.3. Notwithstanding the above, the Data Controller consents to the Data Processor engaging Sub-Processors to process the Personal Data, provided that:

a) the Data Processor shall inform the Data Controller of any planned changes with regard to additions to or replacement of Sub-processors (including details of the processing it performs or will perform) as listed in Appendix B to this DPA; and
b) the Data Processor shall ensure that the Sub-Processor is subject to the same data protection obligations as those specified in this DPA on the basis of a contract or other legal document under the Applicable Data Protection Laws .

6.4. If the Sub-Processor does not fulfil its data protection obligations, the Data Processor shall remain liable to the Data Controller as regards the fulfilment of the obligations of the Sub-Processor.

7. Transfer of data to third countries or international organisations

7.1. Without the approval of the Data Controller, the Data Processor cannot – within the framework of this Data Processing Agreement:

a) disclose Personal Data to a data controller in a third country or in an international organisation;
b) assign the processing of Personal Data to a sub-processor in a third country; or
c) have the data processed in another of the Data Processor's divisions which is located in a third country,

unless otherwise specified within this DPA.

7.2. The Data Controller's instructions or approval of the transfer of Personal Data to a third country, if applicable, shall be set out in Appendix C to this Data Processing Agreement.

7.3. The Data Processor may only process, or permit the processing, of Personal Data outside the UK or

European Economic Area ("**EEA**") under the following conditions:

a) the Data Processor is processing Personal Data in a territory which is subject to a current finding by the European Commission under the Applicable Data Protection Laws that the territory provides adequate protection for the privacy rights of individuals;
b) the Data Processor participates in a valid cross-border transfer mechanism under the Applicable Data Protection Laws, so that the Data Processor (and, where appropriate, the Data Controller) can ensure that appropriate safeguards are in place to ensure an adequate level of protection with respect to the privacy rights of individuals as required by Article 46 of the EU GDPR; or
c) processing is required under the Applicable Data Protection Laws to which the Data Processor is subject. In such a case, the Data Processor shall inform the Data Controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

7.4. To the extent any processing of Personal Data by Data Processor and its Sub-Processors take place in any country outside the UK or EEA (other than exclusively in an Adequate Country), the parties agree that the EC Standard Contractual Clauses approved by the EU authorities under EU Data Protection Laws and set out in Exhibit 1, and as updated from time to time, will apply in respect of that processing and Data Processor will comply with the obligations of the 'data importer' in the EC Standard Contractual Clauses and Data Controller will comply with the obligations of 'data exporter'. By entering into this DPA, the Parties are deemed to be signing the EC Standard Contractual Clauses, as updated from time to time, and its applicable Appendices. The parties agree to enter into any updated EC Standard Contractual Clauses as approved by the EU authorities.

7.5. Should the EC Standard Contractual Clauses or other method applied for cross-border processing under Clause 7.3 cease to be a lawful means of transferring the Personal Data, the parties shall comply with any alternative lawful method of transfer required and complete any documentation required for such alternative lawful method of transfer.

8. Assistance to the Data Controller and Data Subject Rights

8.1. The Data Processor shall, as far as reasonably possible, assist the Data Controller in the fulfilment of the Data Controller's obligations to respond to requests for the exercise of the data subjects' rights including with: the right of access by the data subject, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object and the right to object to the result of automated individual decision-making, including profiling ("**Data Subject Request**").
8.2. Taking into account the nature of the processing, the Data Processor shall provide reasonable assistance at the Data Controller's expense, to the Data Controller by providing appropriate technical and organizational measures, insofar as this is reasonably possible, for the fulfilment of Data Controller's obligation to address any Data Subject Request.

9. Notification of Personal Data breach

9.1. On discovery of a Personal Data breach at the Data Processor's facilities or a Sub-Processor's facilities ("**Security Incident**"), the Data Processor shall as soon as reasonably practicable notify the Data Controller.
9.2. The Data Processor's notification to the Data Controller shall, if possible, take place within forty-eight (48) hours after the Data Processor has discovered the breach to enable the Data Controller to comply with its data breach reporting obligations under (and in accordance with the timescales required by) the Applicable Data Protection Laws.
9.3. The Data Processor shall provide reasonable assistance to the Data Controller in the reporting of the breach to the relevant supervisory authority.

10. Erasure of data

10.1. On termination of the Agreement, the Data Processor shall, at the Data Controller's discretion, return all the Personal Data to the Data Controller and erase existing copies, except to the extent that the Applicable Data Protection Laws require storage of the Personal Data.

11. Inspection and audit

11.1. The Data Processor shall make available to the Data Controller all information reasonably necessary to allow for and contribute to audits, including inspections performed by the Data Controller or another third party auditor mandated by the Data Controller, at the Data Controller's expense, provided that the Data Controller: (i) gives the Data Processor reasonable prior notice of its intention to audit; (ii) conducts its audit during normal business hours; and (iii) takes all reasonable measures to prevent unnecessary disruption to the Data Processor's operations.

11.2. The Data Controller will not exercise its audit rights under this clause 11 more than once in any twelve (12) calendar month period, except (i) if and when required by instruction of a competent data protection authority, or (ii) where the Data Controller believes a further audit is necessary due to a Security Incident by the Data Processor.

11.3. The Data Controller's inspection of sub-processors, if applicable, shall be performed through the Data Processor.

12. Applicability of the CCPA

12.1. To the extent that the Data Processor will process any Personal Data that is subject to the CCPA, the Data Processor shall act as a "service provider," as such term is defined in the CCPA, and shall assist the Data Controller by appropriate technical and organizational measures for the fulfilment of the Data Controller's obligations under the CCPA, including without limitation responding to verified requests by a "consumer," as such term is defined in the CCPA.

12.2. Furthermore, the Data Processor will not engage a Sub-Processor with access to Personal Data except with the Data Controller's prior written consent in accordance with Clause 6 of this DPA and the Data Processor will only do so for a "business purpose," as such term is defined in the CCPA, pursuant to a written contract by and between the Data Processor and such Sub-Processor. Any such approved Sub-Processor shall agree to terms that are at least as protective of Personal Data as the terms of this DPA.

12.3. The Data Processor certifies that it understands it will comply with the responsibilities and restrictions imposed by this DPA as a service provider under the CCPA.

13. The Parties' agreement on other terms

13.1. The consequences of the Parties' breach of this DPA shall be addressed in accordance with the terms of the Agreement.

13.2. In the event of a conflict between this DPA and the data protection provisions within the Agreement (except where explicitly agreed otherwise in writing between the Parties), the terms and conditions set forth in this DPA shall prevail and govern the relationship between the Parties.

14. Commencement and termination

14.1. This DPA shall become effective on the date of both Parties' signature of the Agreement.

14.2. This DPA may be terminated on the basis of the terms specified in the Agreement.

14.3. This DPA shall apply for as long as the processing is performed. Irrespective of the termination of the Agreement and/or this DPA, the DPA shall remain in force until the termination of the processing and the erasure of the data by the Data Processor and any Sub-Processors.

14.4. The DPA and the Agreement shall be interdependent and cannot be terminated separately. The DPA may however – without termination of the Agreement – be replaced by an alternative valid data processing agreement.

15. Governing Law and Jurisdiction

15.1. The Parties to this DPA shall submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity.

15.2. The DPA and all non-contractual or other obligations arising of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Agreement.

16. Severance

16.1. Should any of the provisions of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, preserving the Parties intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part has never been contained therein.

17. Data Processor and Data Controller contacts

17.1. In the event your designated account manager at Fuse cannot assist with a data privacy enquiry, you may contact Fuse's data protection officer at john.taylor@fuseuniversal.com.

17.2. The Parties shall be under obligation continuously to inform each other of changes to contacts/contact

Please sign and return the enclosed copy of this Addendum as instructed to acknowledge the supplementation of these terms to the Agreement.

[Signatures follow on the next page]

CUSTOMER

Customer name (Required): _____

Signature (Required): _____

Name (Required) : _____

Title (Optional) : _____

Date (Required): _____

EU Representative (Required only where applicable): _____

Contact details: _____

Data Protection Officer (Required only where applicable): _____

Contact details: _____

FUSE

Notwithstanding the signatures below of any other Fuse Entity, a Fuse Entity is not a party to this Addendum unless they are a party to the Agreement for the provision of the Software and/or Services to you.

Data Protection Point of Contact: John Taylor
Contact Details: john.taylor@fuseuniversal.com

Fuse Universal Limited:

Signature: _____

Name: _____

Title: _____

Date: _____

Fuse Universal LLC:

Signature:_____

Name: _____

Title: _____

Date: _____

Appendix A Information about the processing

The purpose of the Data Processor's processing of Personal Data on behalf of the Data Controller is:

- The purpose of data processing is to provide learning and training functionality for the Data Controller's users.

The Data Processor's processing of Personal Data on behalf of the Data Controller shall mainly pertain to (the nature of the processing):

- The Data Processor maintains and runs the Fuse service that stores and processes user and learning data.

Processing includes the following categories of data subject:

- Data Controller's employees, contractors.

The Processing concerns the following categories of data:

- Data Controller's employees' data.

The processing includes the following types of Personal Data about data subjects:

The only mandatory user data requirement for Fuse is a unique username for each user on the customer's instance. All other data is optional and defined by the Data Controller. This is typically generic business personal data. For example:

- Personal Data such as:
    - first name/last name
    - username (unique)
    - email address (unique)
    - custom fields such as: location, department, role, hire date, line manager, etc.

In addition, the Data Controller collects the following Personal Data:
Technical data such as:

- IP address
- browser language
- browser type and version
- geolocation
- operating system
- third-party cookie information (where we use third-party services to provide Fuse functionality)

- Fuse activity:
    - login history and transactional activity information (views, likes, shares etc.)
    - training history and learning completions
    - error logs
    - metadata for user-generated content such document uploads and video recordings

The Data Processor's processing of Personal Data on behalf of the Data Controller may be performed when this DPA commences. Processing has the following duration:

- Processing and storage of user data for the term of the Agreement and for the period of sixty (60) days thereafter at which point the Personal Data is destroyed in line with Data Processor's service termination process.

Appendix B Terms of the Data Processor's use of Sub-Processors and list of approved Sub-Processors

B.1 Approved sub-processors

1. Supplier may engage other processors ("**Sub-Processors**") for the Processing of Personal Data under this Data Processing Agreement, provided Supplier ensures such Sub-Processors' compliance with the terms of this Agreement. As of the effective date of the Agreement, the Supplier relies on the Sub-Processors listed in the Order as well as below to provide the Services.

2. Prior to the engagement of another Sub-Processor, the Supplier shall inform your administrator and your contact of the intended Sub-Processing at least thirty (30) days prior thereto, thereby giving you the opportunity to object to such change on reasonable grounds, as set forth in Article 28 of the EU GDPR.

3. You authorize the Supplier to transfer Personal Data to the Supplier's Affiliates and/or other Sub-Processors located in locations outside the UK or European Economic Area, as is reasonably required to provide support, perform technical projects or perform other types of services under the Fuse Master Customer Agreement, provided that, to the extent applicable, either: (i) such locations are recognized by the European Commission as providing adequate data protection; (ii) the Supplier has executed on your behalf the EU Standard Contractual Clauses with such Affiliates and/or other Sub-Processors (you hereby grant such proxy to the Supplier); or (iii) upon your request, you execute the EU Standard Contractual Clauses directly with such Affiliates and/or other Sub-Processors.

4. The Supplier shall remain fully liable to you for the performance of its Sub-Processors' obligations hereunder.

Name	Address	Description of Processing	Legal Basis for Processing
Airbrake USA	228 Hamilton Ave, 3rd Floor Palo Alto, CA 94301	Application exception logging and tracking - Processes in EU & US	Transfers will be based on the adoption of Standard Contractual Clauses (SCCs), as approved under the Commission Implementing Decision (EU) 2021/914, together with a step-by-step implementation of the 01/2020 Recommendations of the EDPB on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data
Amazon Web Services EU	One Burlington Plaza, Burlington Rd, Dublin 4	Processing services - processed in EU West (Dublin, Ireland)	Processed in EU (Dublin, Ireland)
Amazon Web Services USA	410 Terry Avenue North, Seattle, WA 98109-5210, U.S.A.	Hosting and Processing Services - processed in AWS US West (Oregon)	N/A (processed in USA)

Atlassisian	Level 6 341 George Street Sydney, NSW 2000 Australia	Fuse Support Ticketing Support platform- processed in EU West (Dublin, Ireland)	Processed in EU
DataDog	New York Times Bldg, 620 8th Ave 45th Floor New York USA	Logging and Application Performance Monitoring - anonymised data processed in EU & US	Processes in EU and USA
DeepL	DeepL SE, Maarweg 165, 50825 Cologne, Germany	Dynamic translations for platform. Hosted/processed in EEA (Finland)	Processed in EU
Fastly	475 Brannan St. #300 San Francisco, CA 94107	Content Delivery Network – Processes worldwide (Closest POP to connecting users)	Transfers will be based on the adoption of Standard Contractual Clauses (SCCs), as approved under the Commission Implementing Decision (EU) 2021/914, together with a step-by-step implementation of the 01/2020 Recommendations of the EDPB on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data
Fuse Universal LLC	303 Wyman St, Suite 325, Waltham, Massachusetts, 02451	Fuse Subsidiary - processes in US. **Only applicable to Fuse USA customers.**	Processed in USA
Fuse Universal SA (Pty) Ltd	12 Pinewood Rd, Newlands, Cape Town, 7700	Fuse Subsidiary providing customer support and ticketing services – processes in South Africa	Transfers will be based on the adoption of Standard Contractual Clauses (SCCs), as approved under the Commission Implementing Decision (EU) 2021/914, together with a step-by-step implementation of the 01/2020 Recommendations of the EDPB on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data
Good Data	San Francisco 1 Post Street, Suite 400. San Francisco, CA 94104 USA	System Analytics – processed in Rackspace, London	processed in EU
Google	1600 Amphitheatre Parkway in Mountain View, California, United States	GStatic Fonts - Processes in EU and US	Transfers will be based on the adoption of Standard Contractual Clauses (SCCs), as approved under the Commission Implementing Decision (EU) 2021/914, together with a step-by-step

			implementation of the 01/2020 Recommendations of the EDPB on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data
Twilio (Sendgrid)	375 Beale St suite 300 San, Francisco CA 94105 USA	SMTP Relay email notifications - processed EU & US SMS notification relay - processed EU & US	Transfers will be based on the adoption of Standard Contractual Clauses (SCCs), as approved under the Commission Implementing Decision (EU) 2021/914, together with a step-by-step implementation of the 01/2020 Recommendations of the EDPB on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data
UserPilot	1401 Lavaca Street Unit #7019 Austin, TX 78701	In-app analytics for product improvement and innovation (From Q4 2024 replacing Pendo)	Hosted on AWS within EU
StackOne	Camburgh House, 27 New Dover Road, Canterbury, Kent, CT1 3DN, United Kingdom	IPAAS platform for Fuse connectors (3rd party integrations)	Hosted on AWS within EU

Appendix C Instruction pertaining to the use of Personal Data

C.1 The subject of/instruction for the processing

The Data Processor's processing of Personal Data on behalf of the Data Controller shall be carried out by the Data Processor performing the following:
The purpose of data processing is to provide learning and training functionality for the Data Controller's users as described in the Agreement.

C.2 Security of processing

The level of security shall reflect the following:
The Data Processor shall implement the following measures that have been agreed with the Data Controller (on the basis of the risk assessment that the Data Controller has performed):

- Provide mechanisms for the Data Controller to manage and pseudonymise its user data.
- Control unauthorised access to Personal Data and content in line with Data Processor's access control and privacy policies.
- Ensure availability of the platform in line with Data Processor's SLA.
- Provide the level of service, security, auditing and disaster recovery as outlined in Data Processor's ISO27001 policies.

C.3 Storage period/erasure procedures

In line with the Data Processor's service termination process, the Data Processor will destroy all data and content belonging to the Data Controller within the agreed mutually grace period.

C.4 Processing location

Processing of the Personal Data under this DPA cannot be performed at other locations than the following without the Data Controller's prior written consent:

- The Data Controller user data is held, stored and processed in ***the locations stated in Appendix B.***

C.5 Instruction for or approval of the transfer of Personal Data to third countries

- The Data Controller provides instructions and consent pertaining to the transfer of Personal Data to a third country, the Data Processor shall be entitled within the framework of this DPA to perform such transfer.

Appendix D Standard contractual clauses

International transfers, MODULE TWO: Transfer controller to processor

SECTION I

D.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

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 to SCCs.

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

D.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.

D.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

---

[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, 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 2021/915.

(d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

iii. (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.

D.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.

D.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.

D.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 to SCCs.

D.7 *(*optional*)* Docking clause

*(*omitted*)*

2) SECTION II – OBLIGATIONS OF THE PARTIES

D.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 to SCCs, 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 to SCCs. 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 to SCCs. 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 to SCCs.

8.8 Onward transfers

a. 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.

b. 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.

D.9 Use of sub-processors

a. 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 authorisation. The data importer shall submit the request for specific authorisation at least 30 days prior to the engagement of the sub- processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III to SCCs. The Parties shall keep Annex III to SCCs 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[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 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.

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

D.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.

D.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.

D.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.

D.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 to SCCs, 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.

3)

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

D.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.

D.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.

---

[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 timeframe. 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.

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.

5)

6) SECTION IV – FINAL PROVISIONS

D.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.

d. 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.

e. 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.

f. 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.

D.17 Governing law

These Clauses shall be governed by the law of the member state in which the data exporter is established, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the data exporter.

D.18 Choice of forum and jurisdiction

a. Any dispute arising from these Clauses shall be resolved by the courts of a member state in which the data exporter is established.

b. The Parties agree that those shall be the courts of the country where the data exporter is established.

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.

LIST OF PARTIES

See signature page

DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

See Appendix A to DPA.

Categories of personal data transferred

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

See Appendix A to DPA.

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

See Appendix A to DPA.

Nature of the processing

See Appendix A to DPA.

Purpose(s) of the data transfer and further processing

See Appendix A to DPA.

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

See Appendix C to DPA

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

See Appendix B to DPA

COMPETENT SUPERVISORY AUTHORITY

Authority for the member state in which the data exporter is established.

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

The importer shall implement the following technical and organisational measures to ensure security of the data:

See Appendix C to DPA

II. List of Sub-Processors

7) See Appendix B to DPA.