DATA PROCESSING ADDENDUM-PARTNER

BETWEEN:

Partner (hereinafter to be referred to as the "Data Controller"),

AND

HCL Technologies Limited a company duly organized and existing under the laws of India and having its registered offices at 806 Siddharth, 96 Nehru Place, New Delhi-110019; and **HCL America, Inc.**, a California corporation with an office at 330 Potrero Avenue, Sunnyvale, CA 94805 ("Data Processor").

This Data Processing Addendum-Partner ("DPA") is entered into between the above entities and forms a part of and is subject to the agreement ("Agreement") between the parties ("Parties") for the provision of standard software and/or cloud service, software and/or cloud service support and related services (collectively, "Services").

HEREBY AGREE AS FOLLOWS:

1. Subject matter of this Data Processing Addendum

1.1 In the course of providing Services to Data Controller pursuant to the Agreement, Data Processor may process Personal Data that is subject to the European Union's General Data Protection Regulation 2016/679 ("GDPR") or other applicable Data Protection Laws. This Data Processing Addendum reflects the parties' agreement with regard to the processing of such personal data. For the avoidance of doubt, this DPA shall not apply to Partner in its capacity as a reseller of HCL standard software or cloud service.

1.2 "Data Protection Law" means any legislative or regulatory regime enacted by a recognized government, governmental or administrative entity with the purpose of protecting the privacy rights of individuals, to the extent same is applicable to the provision of the Services.

1.3 Terms such as "processing," "personal data," "personal information," "data subject," and "individual" shall have the meaning ascribed to them in the GDPR or the applicable Data Protection Law.

1.4 "Standard Contractual Clauses" or "SCC" means the revised EU standard contractual clauses for the transfer of personal data to third countries published on June 4, 2021, as attached to this DPA as Attachment 2. To the extent Data Controller transfers personal data of UK residents and/or Swiss residents to the Data Processor in a non-adequate third country, then the SCCs shall be deemed to include the UK IDTA attached to the SCC as ANNEX III, and/or the Swiss Amendment attached to the SCC as ANNEX IV, as applicable.

1.5 "US State Data Protection Laws" means comprehensive consumer privacy laws, statutes, rules, requirements and regulations enacted by US states, including without limitation, the California Consumer Privacy Act, the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Connecticut Act Concerning Personal Data Privacy and Online Monitoring, the Utah Consumer Privacy Act, and any comparable legislation in any other states, as each may be amended or replaced from time to time, and any regulations implementing the foregoing.

1.7 Insofar as the Data Processor will be processing personal data subject to the applicable Data Protection Law on behalf of the Data Controller in the course of the performance of the Agreement with the Data Controller, the terms of this Data Protection Addendum shall apply. An overview of the categories of personal data, the types of data subjects, duration and purposes for which the personal data are being processed is provided in Attachment 1.

2. The Data Controller and the Data Processor

2.1 The parties agree, regarding the processing of personal data under GDPR or other applicable Data Protection Laws and this DPA, that (i) Partner determines the purposes and means of processing and is the controller and (ii) HCL is a processor or service provider processing personal data on Partner's behalf. The Parties acknowledge that in some instances the Partner may be acting as a data processor on behalf of a third party, and in such instances, HCL would be the subprocessor. However, for purposes of this DPA and to make this DPA easier to read, the Partner shall be referred to herein as the Data Controller and HCL shall be referred to as the Data Processor.

2.2 The Data Processor will only process the personal data for the purposes of performing the Services under the Agreement and for the purposes set out in this DPA and in the Standard Contractual Clauses or under any other documented instructions from Data Controller, or as required to comply with a legal obligation to which the Data Processor is subject. These instructions are as indicated in the Agreement and the schedules thereto. If the Data Processor must process personal data to comply with a legal obligation in a manner not instructed by Data Controller or otherwise permissible hereunder, the Data Processor shall without undue delay inform the Data Controller of that legal obligation before processing, unless that law explicitly prohibits the furnishing of such information to the Data Controller. The Data Processor shall promptly inform the Data Controller if, in its opinion, an instruction infringes the regulation.

2.3 The Parties have entered into this Data Processing Addendum in order to benefit from the expertise of the Data Processor in securing and processing the personal data for the purposes set out in Attachment 1. The Data Processor shall be allowed to exercise its own discretion in the selection and use of such means as it considers necessary to pursue those purposes, subject to the requirements of this Data Processing Addendum and applicable Data Protection Law.

2.4 Data Controller warrants that it has all necessary rights to provide the personal data to Data Processor for the processing to be performed in relation to the Services. To the extent required by applicable Data Protection Law, Data Controller is responsible for ensuring that it has obtained all necessary data subject consents to this processing, and for ensuring that a record of such consents is maintained. Should such a consent be revoked by the data subject, Data Controller is responsible for communicating the fact of such revocation to the Data Processor, and Data Processor remains responsible for implementing any Data Controller instruction with respect to the further processing of that personal data by Data Processor.

2.5 Data Controller acknowledges that, unless otherwise agreed by the Parties in writing, Data Processor has not requested, does not need, and shall not request access to any personal data (other than business contact data) or any special categories of data or sensitive personal information in performing its obligations under the Agreement or this DPA, and Data Controller agrees to limit the disclosure of such information to Data Processor. Data Controller agrees to mitigate, to the extent practicable, any harmful effect that is known to Data Controller as a result of a use or disclosure of personal data, e.g. by keeping a back up of all personal data submitted.
Data Controller is responsible for ensuring the security of any personal data as it is being disclosed to Data Processor, including the use of encryption in transit.

2.6 Data Processor acknowledges that it will be deemed to be a "Service Provider" under the applicable US State Data Protection Laws with respect to the processing of any personal information. Data Processor shall not "sell" or "share" personal data, as those terms are defined by US State Data Protection Laws. For the avoidance of doubt, Data Processorshall not retain, use, disclose, or Process personal data provided by Data Controller under the Agreement for any purpose, other than as necessary to provide the Services to Data Controller and to perform its obligations under the Agreement, including for Data Processor's own marketing or commercial benefit in any form, or outside of the business relationship between Data Controller and Data Processor. Data Processor further warrants that it shall not combine personal data received from or on behalf of

Data Controller with personal data that it receives from, or on behalf of, another person or persons, or collects from its own interaction with a consumer, except where permitted by Data Protection Law. Data Processor hereby certifies that it understands the restrictions set forth in this Section and will comply with them. Data Processor agrees that it shall promptly inform Data Controller if it makes a determination that it, its subprocessors, or its affiliates can no longer meet their obligations under this Section or under Data Protection Law.

Data Controller discloses personal data to Data Processor solely for: (i) a valid business purpose; and (ii) Data Processor to perform the Services.

3. Confidentiality

3.1 Without prejudice to any existing contractual arrangements between the Parties, the Data Processor shall treat all personal data as confidential and shall inform all its employees, agents and/or approved subprocessors engaged in processing the personal data of the confidential nature of the personal data. The Data Processor shall ensure that all such persons or parties have signed an appropriate confidentiality agreement, are otherwise bound to a duty of confidentiality, or are under an appropriate statutory obligation of confidentiality.

4. Security

4.1 Taking into account the state of the art, the costs of implementation, and the nature, scope, duration, context and purposes of processing as well as the varying likelihood and severity of the risk of harm to the rights and freedoms of individuals and applicable Data Protection Laws, without prejudice to any other security standards agreed upon by the Parties, the Data Controller and Data Processor shall implement technical and organizational measures designed to establish an appropriate level of security for the processing of personal data. The technical and organizational measures of Data Processor ("TOMs") as of the date of this DPA are set forth in the HCLSoftware Trust Center found here: https://www.hcltechsw.com/resources/sw-toms.

4.2 The Data Processor shall at all times have in place an appropriate written security policy with respect to the processing of personal data, outlining in more detail its technical and organizational security measures. At the request of the Data Controller, the Data Processor shall demonstrate the measures it has taken pursuant to Section 4 of this Data Processing Addendum to allow the Data Controller to audit and test such measures.

4.3 The Parties acknowledge that security requirements are constantly changing and that effective security requires frequent evaluation and regular improvements of outdated security measures. The Data Processor will therefore evaluate the measures as implemented in accordance with Section 4 of this Data Processing Addendum on an ongoing basis and will tighten, supplement and improve these measures in order to maintain compliance with the requirements set out in Section 4 of this Data Processing Addendum without compromising or diminishing the security aspect of the Personal Data. The Parties will negotiate in good faith the cost, if any, to implement material changes required by specific updated security requirements set forth in applicable Data Protection Laws or by data protection authorities of competent jurisdiction to the extent same relate to Data Controller's specific use of the Services.

4.4 Where an amendment to the Agreement is necessary in order to execute a Data Controller instruction to the Data Processor to improve security measures as may be required by changes in applicable Data Protection Law from time to time, the Parties shall negotiate an amendment to the Agreement in good faith.

5. Audit rights

5.1 Subject to this Section 5, Data Processor shall:

a) make available to the Data Controller on the provision of not less than thirty (30) days written notice, all relevant information necessary to demonstrate compliance with this Agreement, or

b) allow for and contribute to an audit, by the Data Controller or an auditor mandated by the Data Controller, in relation to the processing of the personal data in accordance with the Agreement.

5.2 Any audit under 54.1(b) will be subject to the following conditions:

a) The scope, content and timing of the proposed audit shall be agreed between the parties in advance;

b) any third party auditor appointed by Data Controller must be independent of the parties and not be a competitor of Data Processor;

c) auditors must be bound by a confidentiality agreement provided by Data Processor;

d) the cost of any audit will be borne by the Data Controller; and

e) audits will not take place on Data Processor's premises and more frequently than once within a twelve (12) month period or as otherwise expressly agreed between the parties in response to a breach or other data privacy incident.

6. Data Transfers

6.1 To the extent Data Controller transfers personal data of EU residents to the Data Processor located in a non-EU country or a country not deemed adequate under applicable laws, such transfers shall be governed by and under the SCCs attached to this DPA as Attachment 2.

To the extent Data Controller transfers personal data of UK residents to the Data Processor located in a non-EU country or a country not deemed adequate under applicable laws, such transfers shall be governed by and under the SCCs as further amended by the UK IDTA attached to the SCCs as ANNEX III.

To the extent Data Controller transfers personal data of Swiss residents to the Data Processor located in a non-EU country or a country not deemed adequate under applicable laws, such transfers shall be governed by and under the SCCs as further amended by the Swiss amendment to the SCCs as ANNEX IV.

Signature of this DPA constitutes signatures to the SCCs including the annexes thereto.

6.2 The Data Processor hereby notifies the Data Controller of, and the Data Controller hereby consents to, processing of personal data by affiliates and third party subprocessors (in accordance with Section 8 below) as set forth in the HCLSoftware Trust Center found at https://www.hcltechsw.com/resources/trust-center. HCL as the Data Processor is executing the SCC with such subprocessors as adequate safeguards where appropriate or required by applicable Law. The Data Controller hereby agrees to such personal data transfers, including the use of SCCs, under this Agreement.

6.3 To the extent that the Data Controller or the Data Processor are relying on a specific statutory mechanism to normalize international data transfers that is subsequently modified, revoked, or held in a court of competent jurisdiction to be invalid, the Data Controller and the Data Processor agree to cooperate in good faith to promptly terminate the transfer or to pursue a suitable alternate mechanism that can lawfully support the transfer.

7. Information Obligations and Incident Management

7.1 Incidents. When the Data Processor becomes aware of a successful incident that impacts the processing of the personal data that is the subject of the Agreement, it shall notify the Data Controller about the incident without undue delay after confirmation of the incident, shall at all times cooperate with the Data Controller, and shall follow the Data Controller's instructions with regard to such incidents, in order to enable the Data Controller to perform a thorough investigation into the incident, to formulate a correct response, and to take suitable further steps in respect of the incident.

7.2 The term "incident" used in Section 7.1 of this Data Processing Addendum shall be understood to mean in any case:

7.2.1 a request for access to personal data provided hereunder by Data Controller to Data Processor by government officials or law enforcement entities. In the event that Data Processor receives such a request, Data Processor will notify Data Controller of such request to enable Data Controller to take all necessary actions to communicate directly with the relevant authority and respond to such request. If Data Processor is prohibited by law from notifying Data Controller of such request, then where it will believes such a request is invalid or unlawful, it will try to challenge it. If the government official or law enforcement entities persist with a valid request, Data Processor will use reasonable efforts to limit the personal data it provides to the specific data elements necessary to legally meet the requirements of the request.

7.2.2 any unauthorized or accidental access, processing, deletion, loss or any form of unlawful processing of the personal data;

7.2.3 any breach of the security and/or confidentiality as set out in Sections 3 and 4 of this Data Processing Addendum leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, the personal data;

7.2.4 where, in the opinion of the Data Processor, implementing an instruction received from the Data Controller would violate applicable laws to which the Data Controller or the Data Processor are subject.

7.3 The Data Processor shall at all times have in place written procedures which enable it to promptly respond to the Data Controller about an incident. Where the incident is reasonably likely to require a data breach notification by the Data Controller under applicable Data Protection Law, the Data Processor shall implement its written procedures in such a way that it is in a position to notify the Data Controller no later than seventy-two (72) hours of having confirmed such an incident.

7.4 Any notifications made to the Data Controller pursuant to this Section 7 of this Data Processing Addendum shall be addressed to the employee of the Data Controller whose contact details are provided in Section 13 of this Data Processing Addendum, and shall contain, to the extent such information is available to Data Processor:

- a description of the nature of the incident, including where possible the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- the name and contact details of the Data Processor's data protection officer or another contact point where more information can be obtained;
- a description of the likely consequences of the incident; and
- a description of the measures taken or proposed to be taken by the Data Processor to address the incident including, where appropriate, measures to mitigate its possible adverse effects.

7.5 Data Subject Requests. If Data Processor receives a request from a data subject to exercise his or her right of access, right to rectification, restriction of processing, erasure, data portability objection to further processing or the right not to be subject to automated individual decision making, or any other rights provided to individuals under applicable Data Protection Laws, the Data Processor will, to the extent legally permitted, promptly forward such request to the Data Controller. Except to the extent required by applicable Data Protection Law, Data Processor shall not respond to any such request without Data Controller's explicit instruction, except to confirm receipt of the request and confirm that the request relates to Data Controller.

8. Contracting with Subprocessors

8.1 The Data Controller authorizes the Data Processor to engage subprocessors set forth in the HCLSoftware Trust Center found at https://www.hcltechsw.com/resources/trust-center. Data Controller may subscribe to receive updates to the subprocessors on the HCLSoftware Trust Center website. If Data Controller wishes to object to a new subprocessor on the reasonable basis that the subprocessor is not able to adequately protect the personal data, Data Controller shall contact the Data Controller's account manager at Data Processor within thirty (30) days of being notified of such change in subprocessors.

8.2 The Data Processor shall ensure that each subprocessor is bound by the same or similar data protection obligations of the Data Processor under this Data Processing Addendum. Data Processor shall be liable for the acts and omissions of its subprocessors to the same extent Data Processor would be liable if performing the services of each subprocessor directly under the terms of this DPA.

9. Return or Destruction of Personal Data

9.1 At the Data Controller's written request, within forty-five (45) days of termination or expiration of the applicable Agreement and fulfillment of the purposes agreed in the context of the Services (or as otherwise agreed by the parties) the Data Processor shall either delete, destroy or return all files containing personal data provided to Data Processor under the Agreement to the Data Controller and destroy or return any existing copies. Consideration shall be taken at such time as to whether there is any legitimate need to retain the personal data so as not to disrupt any operations or otherwise interfere with the Services provided hereunder. Notwithstanding the above, personal data shall not be retained for longer than permitted under applicable laws.

9.2 HCL may temporarily retain one copy of personal data made for backup or archival purposes in the ordinary course; provided that such backup or archival copy will be subject to the ongoing obligations contained herein and shall be destroyed upon the normal expiration of backup or archival files. Further, if any law, regulation, or government or regulatory body requires HCL to retain any documents or materials that HCL would otherwise be required to return or destroy, then HCL may retain such documents and/or materials. HCL may only use this retained personal data for the required retention reason or audit purposes.

9.3 Upon such deletion in accordance with Section 9.1 above, the Data Processor shall, as appropriate, notify third parties to whom it has transferred personal data and request that the personal data be deleted from any third parties platforms, including any subprocessors' platforms.

10. Assistance to Data Controller

10.1 Taking into account the nature of the processing and the information available to the Data Processor, the Data Processor shall assist the Data Controller insofar as this is feasible, for the fulfilment of the Data Controller's obligation to respond to requests for exercising the data subject's rights under the Data Protection Laws.

10.2 The Data Processor shall assist the Data Controller in ensuring compliance with the obligations

pursuant to Section 4 (Security) of this Data Processing Addendum and prior consultations with supervisory authorities required under Article 36 of the GDPR taking into account the nature of processing and the information available to the Data Processor.

10.3 The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with the Data Processor's obligations and allow for and contribute to audits, per the terms of the Agreement and this DPA. The Data Processor shall assist the Data Controller in ensuring compliance with the obligations pursuant to Clause 35 of the GDPR.

11. Duration and Termination

11.1 This Data Processing Addendum shall come into effect as of the effective date of the applicable Agreement that governs the support and maintenance and/or professional services provided by Data Processor to Data Controller. The Data Processor shall process personal data until the date of termination of the Agreement, subject to Section 9.

11.2 Termination or expiration of the Agreement and this Data Processing Addendum shall not discharge the Data Processor from its confidentiality obligations pursuant to Section 3 of this Data Processing Addendum.

12. Miscellaneous

12.1 In the event of any inconsistency between the provisions of this Data Processing Addendum and the provisions of the Agreement, the provisions of this Data Processing Addendum shall prevail.

12.2 Data Controller shall not unreasonably withhold or delay agreement to any consequential variations to this Addendum proposed by Data Processor to protect the Data Processor against additional risks associated. If Data Controller proposes any other variations to this Addendum which Data Controller reasonably considers to be necessary to address the requirements of any Data Protection Law, the parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in Partner's notice as soon as is reasonably practicable.

12.3 Each party's liability arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' or similar provision of the Agreement governing the applicable Programs and Services.

12.4 This Data Processing Addendum is governed by the laws of the applicable Member State where the personal data is processed. Any disputes arising from or in connection with this Data Processing Addendum shall be brought exclusively before the competent court of the applicable Member State where the personal data is processed.

12.5 The Parties agree to execute the below addenda as required.

13. Contact Information

Data Controller	**Data Processor**	
	HCLSoftware	**HCLTechnologies**

The **primary contact** as provided by the Data Controller or as specified here: _____. If not specified, this will be the main Partner contact.	**Chief Privacy Officer** 2600 Great America Way, Suite 101 and 401, Santa Clara, CA 95054 **USA** hclswprivacy@hcl-software.com	**Chief Privacy Officer** Axon Centre, Church Road Egham, TW20 9QB England **UK** privacy@hcltech.com

114. Signatures

	Customer	**HCL Technologies Limited**
Signature:	_____	_____
Name:	_____	_____
Date:	_____	_____
		HCL America, Inc.
Signature:	_____	_____
Name:	_____	_____
Date:	_____	_____

Attachment 1

Personal data that will be processed in the scope of and for the duration of the Agreement and the purposes for which the personal data will be processed.

Personal data shall be used for the purpose of providing the Services set forth in the Agreement. Personal data processed under this DPA is limited to the following types of personal data:

Partner Contact Information: To communicate with the Partner, HCL support team maintains a record of Company and Contact details that include, but is not limited to, Company Name, Company address, Contact Name, email address, and telephone number.

Case data including Partner Contact Information: The Support case data would be any information that the Partner enters in the support portal itself during the lifetime of the case (i.e. description of their problem, communication back and forth with HCL support team to troubleshoot the issue).

Diagnostic data: To work on Partner support queries, information between the Partner and HCL Support needs to be shared. Partner may upload data, like log and configuration files, for HCL support team to use in troubleshooting reported problems.

Special Categories of Data and other sensitive personal information should never be provided under this Agreement.

Contact information and data received from Partner and/or third parties: By providing access to cloud based services, HCL will process personal information received from data subjects such as names, email addresses, phone numbers, device identifiers and static IP addresses. Personal data should not be entered into fields that do not require it. Cloud services are not designed to process special categories of personal data. Cloud Services involves the processing of data provided by Partners and/or Customers including data transmission, data retrieval, data access and network access to allow transfer of data as needed, transition of data as required to deliver the Cloud Service and storage and deletion of data as required.

Other Personal Data not included above: Given the enterprise nature of any Cloud Services that may be provided, Partner must acknowledge and shall ensure that the Customer acknowledges, that HCL cannot verify or maintain complete list of types of personal data, special categories of personal data and data subjects. If Partner and/or Customer uses Cloud Services in such a way that data beyond that envisaged above, then Partner and/or Customers are responsible for providing complete, accurate, and up-to-date information to HCL on the actual types of personal data and special categories of personal data that the Partner and/or Customer will process using Cloud Services by providing additional instructions separately.

Attachment 2

HCL EU STANDARD CONTRACTUAL CLAUSES

(for Personal Data exported from the EU/EEA including the ANNEXES III for the UK and IV for Switzerland, as applicable)

published June 4th, 2021

Modules 2 (Controller to Processor) and 3 (Processor to Processor)

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

(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.

[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 […].

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

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7 - Optional

Docking clause

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

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

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

MODULE TWO: Transfer controller to processor

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;

[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.

(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

(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.

MODULE THREE: Transfer processor to processor

8.1 Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter[3].

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 controller, as communicated to the data importer by the data exporter, or 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 personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand 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.

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 rectify or erase 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 controller 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

[3] See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.

the appropriate level of security, they 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 subject. 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 or the controller. 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 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, without undue delay, the data exporter and, where appropriate and feasible, the controller 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 data breach, including 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 its controller so that the latter may in turn 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 set out 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 controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[4] (in the same country as the data

[4] 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

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 of Regulation (EU) 2016/679;

(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

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller 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 controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) 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.

(g) 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

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 purposes of these Clauses.

MODULE TWO: Transfer controller to processor

(a) OPTION 2: GENERAL WRITTEN AUTHORISATION 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 thirty (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.[5] 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.

MODULE THREE: Transfer processor to processor

(a) OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the controller 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 controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), 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.[6] The Parties agree that, by

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

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

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

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

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

Clause 10

Data subject rights

MODULE TWO: Transfer controller to processor

(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.

MODULE THREE: Transfer processor to processor

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. 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 controller, as communicated by the data exporter.

Clause 11

Redress

(d) 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.

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) 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.

(b) 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.

(c) 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.

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

(e) 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

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(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

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] 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.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, 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

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(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[7];

[7] 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

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

(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 [for Module Three: , if appropriate in consultation with the controller]. 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 [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

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

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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

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.

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.

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

(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. [For Module Three: The data exporter shall make the assessment available to the controller.]

(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) [For Modules One, Two and Three: 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.] [For Module Four: Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.] 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

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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

Clause 18

Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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

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

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

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

APPENDIX TO THE STANDARD CONTRACTUAL CLAUSES

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

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

If not specified here, this shall be the information of the Data Controller

Name: …

Address: …

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

Activities relevant to the data transferred under these Clauses: …

Signature and date: …

Role: Controller or Processor, as applicable

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

Name: HCLSoftware entity as the Licensor as defined in the main Agreement

Address: …

Contact person's name, position and contact details:

see Section 13 of the DPA; Email: hclswprivacy@hcl-software.com

Activities relevant to the data transferred under these Clauses: see main Agreement

Signature and date: …

Role: Processor or Sub-Processor, as applicable

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

The personal data transferred concern the following categories of data subjects (please specify):

Data exporter may submit Personal Data to the Data Importer, the extent of which is generally determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to, Personal Data relating to the following categories of data subjects:

- Data exporter's employees
- End users of the application associated with the software product
- Any other data subjects as defined by data exporter based on the business use cases which utilize the software product

Categories of personal data transferred

The personal data transferred concern the following categories of data (please specify):

- Contact details (includes but is not limited to Contact name, business phone number, business email address, Contact's timezone, etc.)
- Profile details (includes but is not limited to business details such as job title, location, etc. required to interact with the software product)
- Any other categories of data reasonably expected to be provided in the Service based on the business use cases which utilize the software product

Special Categories of Data* (if appropriate***)**

The personal data transferred concern the following special categories of data (please specify):

N/A

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

The frequency is dependent on the nature of the services provided by Data Processor.

Nature of the processing

The nature of the processing is described in the applicable agreement between the parties.

Purpose(s) of the data transfer and further processing

The purpose of the data transfer is described in the Data Processing Agreement.

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

Personal data will be retained as specified in the Data Processing Agreement and only to the extent permitted by applicable law.

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

The subject matter, nature and duration of processing by subprocessors is described in the Data Processing Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

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

Ireland

ANNEX II

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

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Taking into account the state of the art, the costs of implementation, and the nature, scope, duration, context and purposes of Processing as well as the varying likelihood and severity of the risk of harm to the rights and freedoms of individuals and applicable Data Protection Laws, without prejudice to any other security standards agreed upon by the Parties, the Data Importer shall implement technical and organizational measures designed to establish an appropriate level of security for the Processing of Personal Data. These technical and organizational measures are set forth here: https://www.hcltechsw.com/resources/sw-toms.

ANNEX III

UK INTERNATIONAL DATA TRANSFER ADDENDUM (or "UK IDTA")
(for Personal Data exported from the UK)

The following UK International Data Transfer Addendum (Version B1.0 published March 21, 2022) shall apply to the extent that this Agreement involves a restricted transfer of personal data from the UK.
The parties hereto agree to modify the above EU Commission Standard Contractual Clauses to address the transfer of UK personal data as follows:

The Information Commissioner considers this Addendum to provide appropriate safeguards for restricted transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date	Per the Agreement	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	As defined in the Agreement	As defined in the Agreement
Key Contact	Full Name (optional): Job Title: Contact details including email:	Full Name (optional): as defined in the Agreement Job Title: as defined in the Agreement Contact details including email: hclswprivacy@hcl-software.com
Signature (if required for the purposes of Section 2)	_____	_____

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☒ The version of the Approved EU SCCs which this Addendum is appended to, including the Appendix Information.

Table 3: Appendix Information

"**Appendix Information**" means the information set out in the Updated SCCs as set forth below:

Annex 1A: List of Parties: Per Annex I of the EU SCC above
Annex 1B: Description of Transfer: Per Annex I of the EU SCC above
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: Per Annex II of the EU SCC above
Annex III: List of Sub processors (Modules 2 and 3 only): As set forth on Licensor's Trust Center found here [https://www.hcltechsw.com/resources/data-processing-and-transfers] as may be updated from time to time. Customer may subscribe to receive updates in accordance with clause 9 (a) Option 2 of the Updated SCCs.

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☐ Importer ☐ Exporter ☒ neither Party

Part 2: Mandatory Clauses:

Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

ANNEX IV

Swiss Addendum to the Standard Contractual Clauses for the Transfer of Personal Data from the Swiss Confederation to Third Countries

If Personal Data falls within the scope of Swiss Data Protection Law and is transferred to a third country that does not ensure an adequate level of data protection under Swiss Data Protection Law, the Parties will agree that the Standard Contractual Clauses at **Attachment 2** to the DPA will apply, as amended in accordance with the Swiss Federal Act on Data Protection ("CH-DPA") with the following prevailing provisions so as to comply with the Swiss Federal Data Protection and Information Commissioner ("**FDPIC**") issued guidance approving the use of the Standard Contractual Clauses:

(a) The Parties adopt the standard of the Regulation (EU) 2016/679 for all Restricted Swiss Data Transfers .

(d) Competent supervisory authority (Clause 13):

(i) To the extent the transfer of personal data is governed by the CH-DPA, the FDPIC shall act as the competent supervisory authority.

(ii) To the extent the transfer of personal data is governed by the Regulation (EU) 2016/679, the Irish Data Protection Commission shall act as the competent supervisory authority.

(e) Governing law (Clause 17): These Clauses shall be governed by the laws of Ireland as determined in Clause 17 of the Standard Contractual Clauses at Exhibit 1.

(f) Choice of forum and jurisdiction (Clause 18.a/b): Any dispute arising from these Clauses shall be resolved by the courts of Ireland as determined in Clause 18.b of the Standard Contractual Clauses at Exhibit 1.

(g) Data subject jurisdiction (Clause 18.c): The term "Member State" shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of pursuing their rights at their place of habitual residence (Switzerland) in accordance with Clause 18.c of the Standard Contractual Clauses at Exhibit 1. Accordingly, data subjects with their place of habitual residence in Switzerland may also bring legal proceedings before the competent courts in Switzerland.

(h) Scope of "personal data" (Clause 1.a/c): In addition to personal data pertaining to natural persons, these Clauses shall be applicable to and protect personal data pertaining to legal entities as well, if and to the extent such personal data pertaining to legal entities is within the scope of the CH-DPA.

(i) The Parties agree to bound by this Swiss Addendum to the Standard Contractual Clauses and its requirement upon execution of the Addendum, and that no additional signatures are required to make this Swiss Addendum to the Standard Contractual Clauses enforceable and binding upon the Parties.