

Contents of the DPA	Page
1. Introduction	1
2. Definitions	1
3. Processing Operations	3
4. Processing Obligations	3
5. Data Subject Rights	4
6. Data Protection Impact Assessment	4
7. Sub-Processing	4
8. Data Transfers	5
9. Audit	5
10. Security and Breach (Including Supplementary Measures)	6
11. Limitation of Liability	7
12. Governing Law, Competent Jurisdiction and Hierarchy	7
Signatures	7
Annex 1 to the DPA – Details of Processing of Customer Personal Data	8
Annex 2 to the DPA – Security of Processing	10
Annex 3A to the DPA – 2021 Model Clauses (for EU/EEA & Swiss Data Exporters)	11
Appendix to the 2021 Model Clauses	25
Annex I to the 2021 Model Clauses	25
Annex II to the 2021 Model Clauses	27
Third-Country Addendum to the 2021 Model Clauses: Switzerland	28
Annex 3B to the DPA – International Data Transfer Amendment (for UK Data Exporters)	29
	37
	38

## 1. Introduction

This Data Processing Addendum (“DPA”) is entered into by the entity identified in the signature box below (“Customer”) and the Regional CA Entity, a Broadcom Inc. company, (“CA”) and forms part of the agreement between CA and Customer for CA to provide Services (“Agreement”) to Customer.

In the course of providing Services to Customer pursuant to the Agreement, CA may Process Customer Personal Data that is subject to the European Union’s General Data Protection Regulation, Regulation (EU) 2016/679 (“GDPR”) or other Data Protection Laws. This DPA reflects the parties’ agreement with regard to the Processing of such Customer Personal Data. For purposes of this DPA CA is the Processor and Customer is the Controller.

The parties agree to comply with the following provisions, each acting reasonably and in good faith.

## 2. Definitions

**“Affiliates”** means any entity which directly or indirectly owns, controls, is controlled by, or is under common control with a party, where control is defined as owning or directing more than fifty percent (50%) of the voting equity securities or a similar ownership interest in the controlled entity.

**“Agreement”** means all current and future agreements between CA and Customer in connection with which CA provides Services involving the Processing of Personal Data on behalf of Customer. This DPA is incorporated into such Agreements by this reference.

**“Controller”** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data;

## Data Processing Addendum

**“Data Protection Laws”** means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland and the United Kingdom including the GDPR, applicable to the Processing of Personal Data under the Agreement.

**“International Data Transfer Addendum (IDT)”** means the addendum to the EU Commission Standard Contractual Clauses, version B1.0, in force 21 March 2022, which has been issued by the Information Commissioner for Parties making Restricted Transfers and incorporated as Annex 2B to this DPA.

**“Regional CA Entity”** shall mean, depending on the CA entity that is a party to the Agreement, CA, Inc., 1320 Ridder Park Drive, San Jose, CA 95131 (North America) or CA Europe Sarl Route de la Longeraie 7, 1110 Morges Switzerland (Europe, Middle East and Africa) or CA Programas de Computador, Avenida Dr. Chucuri Zaidan, 1240 – 27º andar, Golden Tower, CEP 04711-130 - São Paulo-SP, Brazil - CNPJ/MF 08.469.511/0001-69 (Latin America) or CA (Singapore) Pte Ltd., 1 Yishun Avenue 7, Singapore, 768923 (Asia, Pacific and Japan).

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

**“Personal Data Breach”** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.

**“Processing”** (and its cognates), means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

**“Processor”** means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

**“Services”** means the provision of maintenance and support services and/or the provision of software as a service (“SaaS”) and/or any other services, hosted, managed or otherwise, which are provided under the Agreement and for the purposes of which CA Processes Personal Data on behalf of Customer.

**“Model Clauses”** means the agreement pursuant to the European Commission’s decision (EU) 2021/914 of 4 June 2021 (Commission Implementing Decision (EU) 2021/914 on Standard Contractual Clauses (“2021 Model Clauses”) for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council as officially published at <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914&from=EN>.

**“Supervisory Authority”** means an independent public authority which is established under applicable Data Protection Laws.

**“Sub-Processor”** means a Processor which Processes Personal Data on behalf of another Processor.

**“CA Sub-Processor”** means any first-party and third-party Sub-Processor engaged by CA or its Affiliates.

### 3. Processing Operations

- a) The subject matter and duration of the Processing of Personal Data are set out in the Agreement, which describes the provision of the Services to Customer. The nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects are set forth in Annex 1 to this DPA (titled “Annex 1: Details of Processing Customer Personal Data”).
- b) In its Processor capacity, CA shall only Process Personal Data on behalf of and in accordance with Customer’s documented instructions. The Agreement (including this DPA) constitutes such documented initial instructions and each use of the Services then constitutes further instructions. CA will use reasonable efforts to follow any other Customer instructions, as long as they are required by Data Protection Laws and technically feasible.
- c) As part of the configuration of the Services, certain security features and data Processing functionalities are made available to Customer. Customer is responsible for properly configuring the Services to meet its specific Processing and security requirements, which may include use of pseudonymization and/or encryption technologies and of any other such information security and/or privacy enhancing measures as Customer deems appropriate to protect the Personal Data from unauthorized Processing.
- d) Customer is responsible for the accuracy, quality, and legality of the Personal Data, and the means by which Customer acquired the Personal Data.

### 4. Processing Obligations

When providing the Services, CA shall:

- a) Process such Personal Data in compliance with Customer’s instructions as set forth in the parties’ Agreement for Services, including with regard to transfers of Personal Data to a third country or international organization, unless other Processing is required by applicable Data Protection Laws, in which case CA shall inform Customer of that legal requirement before Processing unless the law prohibits such notice on important public-interest grounds;
- b) Ensure that CA personnel authorized to Process such Personal Data have committed themselves to confidentiality requirements at least as protective as those of this DPA or the Agreement governing the applicable engagement with CA for which Processing is performed or are under an appropriate statutory obligation of confidentiality;
- c) Implement appropriate technical and organizational measures to protect such Personal Data in accordance with applicable Data Protections Laws, taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons; as set forth in Annex 2 - Security of Processing
- d) Taking into account the nature of the Processing and the information available to CA, assist Customer in ensuring compliance with Customer’s obligations pursuant to Articles 32 to 36 of the GDPR and in accordance with applicable Data Protections Laws;
- e) Upon termination of the parties’ Agreement and/or after the end of provision of the Services to which this DPA applies, delete or return any Customer Personal Data in accordance with Data Protection Laws and/or consistent with the terms of the Agreement as soon as reasonably practicable, unless applicable law requires further storage;



## Data Processing Addendum

- f) Inform Customer if CA cannot comply with an instruction or in CA's opinion, a Customer instruction infringes applicable Data Protection Laws.

### 5. Data Subject Rights

- a) Taking into account the nature of the Processing, CA shall use appropriate technical and organizational measures insofar as possible to assist Customer in fulfilling Customer's obligation to respond to requests for the exercise of Data Subject rights in accordance with applicable Data Protections Laws.
- b) CA shall, to the extent legally permitted, promptly notify Customer if it receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure, data portability, objection to further Processing, or its right not to be subject to automated individual decision making ("Data Subject Request"). Except to the extent required by applicable law, CA shall not respond to any such Data Subject Request without Customer's prior written authorization or explicit instruction, except to confirm that the request relates to Customer.

### 6. Data Protection Impact Assessment

- a) CA shall provide Customer with reasonable assistance as needed to fulfil Customer's obligation to carry out a data protection impact assessment as related to Customer's use of the Services. CA will provide such assistance upon Customer's reasonable request and to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to CA.
- b) CA shall provide Customer with reasonable assistance in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to this Section 6 and to the extent required under applicable Data Protection Laws.

### 7. Sub-Processing

- a) CA is granted a general authorization to subcontract the Processing of Personal Data to CA Sub-Processors. CA shall enter into a written agreement with any such CA Sub-Processor that Processes Customer Personal Data which imposes obligations on the CA Sub-Processor no less protective than those imposed on CA under this DPA.
- b) CA shall remain liable to Customer for the performance of CA Sub-Processors' obligations with respect to Customer Personal Data in accordance with the terms of this DPA. The list of CA Sub-Processors used by CA in connection with its provision of the Services is available at: <https://www.broadcom.com/company/legal/privacy/sub-processors>. In the event CA makes any changes or additions to such list, CA shall provide notice through the current CA Sub-Processor List made available to Customer at: <https://www.broadcom.com/company/legal/privacy/sub-processors> or through email where Customer has subscribed under <http://learn.broadcom.com/subprocessor-news-opt-in> for notification. Customer may object to such changes as set forth in subsection c) below.
- c) Customer may object to CA's use of a new CA Sub-Processor by notifying CA promptly in writing within thirty (30) calendar days after any updates are made by CA to the CA Sub-Processor list or Customer has been notified by email. In the event of such objection by Customer, CA will take

## Data Processing Addendum

commercially reasonable steps to address the objections raised by Customer and provide Customer with reasonable written explanation of the steps taken to address such objection.

### 8. Data Transfers

- a) CA will abide by the requirements of European Economic Area, the United Kingdom and Swiss data protection laws regarding the collection, use, transfer, retention, and other Processing of Personal Data from the European Economic Area, the United Kingdom and Switzerland. Solely for the provision of Services to Customer under the Agreement, Personal Data may be transferred to and stored and (or) Processed in any country in which CA or its CA Sub-Processors operate. Customer instructs CA to perform any such transfer of Personal Data to any such country and to store and Process Personal Data to provide the Services. All transfers of Personal Data out of the European Union, European Economic Area, United Kingdom and Switzerland shall be governed by the relevant Model Clauses which the parties hereby enter into and incorporate to this DPA by the aforementioned reference, or be subject to appropriate safeguards in accordance with applicable Data Protections Laws.
- b) If transfers of EU/EEA, Swiss or UK Data are executed by relying on the Model Clauses – in which case, as relevant, the Parties hereby agree to enter into the above-referenced Model Clauses and to incorporate them as Annexes 3A and/or 3B to this DPA, using the 2021 Model Clauses as they pertain to transfers from the EU/EEA and Switzerland (Annex 3A below) and the IDT as it pertains to transfers from the UK (Annex 3B below), with Customer as Data Exporter and CA as Data Importer –, CA shall at all times comply with (and ensure that all Subcontractors comply with) the Model Clauses and/or the IDT. For the purposes of the 2021 Model Clauses, Module 2 shall apply by default with Customer as Controller and CA as Processor, unless the Parties explicitly agree that Module 3 shall apply with Customer as Processor and CA as Sub-Processor.
- c) CA and CA Affiliates acting as CA Sub-Processors have previously entered into the Model Clauses for the benefit of Customer.
- d) In the event of a conflicting clause between any term or Annex of this DPA and the Model Clauses or IDT, the Model Clauses or IDT shall prevail. For the avoidance of doubt, where this DPA further specifies sub-processing and audit rules in Sections 7 and 9, such specifications also apply in relation to the Model Clauses and IDT and shall only supplement them.

### 9. Audit

- a) CA shall make available to Customer, upon reasonable written request, information related to the Processing of Personal Data of Customer as necessary to demonstrate CA's compliance with the obligations under this DPA. CA shall allow for inspection requests by Customer or an independent auditor in relation to the Processing of Personal Data to verify that CA's is in compliance with this DPA, if (a) CA has not provided sufficient written evidence of its compliance with the technical and organizational measures, e.g. a certification of compliance with ISO 27001 or other standards; (b) a Personal Data Breach has occurred; (c) an inspection is officially requested by Customer's Supervisory Authority; or (d) Data Protection Law provides Customer with a mandatory on-site inspection right; and provided that Customer shall not exercise this right more than once per year unless mandatory Data Protection Law requires more frequent inspections. Any information provided by CA and/or audits performed pursuant to this section are subject to the confidentiality obligations set forth in the Agreement. Such inspections shall be conducted in a manner that does not impact the ongoing safety, security, confidentiality, integrity, availability, continuity and

## Data Processing Addendum

resilience of the inspected facilities, networks and systems, nor otherwise expose or compromise any confidential data Processed therein.

- b) Customer is responsible for all costs associated with any such audit or inspection, including reimbursement of CA for all reasonable costs of complying with Customer or regulator instructions, unless such audit reveals a material breach by CA of this DPA, then CA shall bear its own cost of such an audit. If an audit determines that CA has breached its obligations under this DPA, CA will promptly remedy the breach at its own cost.

### 10. Security and Breach (Including Supplementary Measures)

- a) CA shall implement appropriate technical and organizational measures to protect Customer Personal Data in accordance with applicable Data Protections Laws taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons and as set forth in Annex 2 - "Security of Processing".
- b) **Supplementary Measures:** In order to maintain the protection of Personal Data granted in the European Economic Area ("EEA"), CA shall collaborate with Customer in the event of international data transfers from the EEA to the United States. For the appropriate safeguards contained in the GDPR Article 46 transfer tools to be effective, CA shall comply with the following supplementary measures. It undertakes (i) to provide encryption key management as outlined in the security controls referenced in Annex 2 - "Security of Processing"; (ii) to challenge unjust government data access request to Customer Personal Data if any; and (iii) to delete any Customer Personal Data as soon as reasonably practicable after the Agreement has ended, unless CA has valid legal reasons for retaining such data for longer.
- c) CA shall notify Customer without undue delay after becoming aware of any Personal Data Breach involving such Customer Personal Data Processed by CA; CA will use reasonable efforts to identify the cause of such Personal Data Breach and shall without undue delay: (a) investigate the Personal Data Breach and provide Customer with information about the Personal Data Breach, including if applicable, such information a Data Processor must provide to a Data Controller under Article 33(2) of the GDPR to the extent such information is reasonably available; and (b) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Personal Data Breach to the extent the remediation is within CA's reasonable control. Notification will be delivered to Customer in accordance with subsection e) below.
- d) CA's obligation to report or respond to a Personal Data Breach under this Section is not and will not be construed as an acknowledgement by CA of any fault or liability with respect to the Personal Data Breach.
- e) Notification(s) of Personal Data Breaches, if any, will be delivered to one or more of Customer's business, technical or administrative contacts, designated by Customer in the Order Form or Support Portal, by any means CA selects, including via email. It is Customer's sole responsibility to ensure it provides and maintains accurate and current contact information at all times.

### 11. Limitation of Liability

Each party's and all of its Affiliates' liability, taken together in the aggregate, 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'





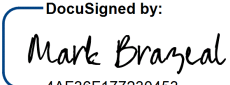

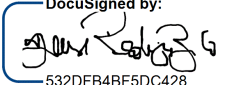
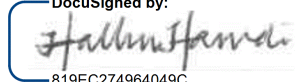
## Data Processing Addendum

section of the Agreement governing the applicable Services, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together. For the avoidance of doubt, each reference to the DPA in this DPA means this DPA including its Annexes, Schedules and/or Appendices.

### 12. Governing Law, Competent Jurisdiction and Hierarchy

The applicable law and competent courts for this DPA are those of the main Agreement which this DPA attaches to. If there is any conflict or inconsistency between this DPA and the Agreement, this DPA shall prevail to the extent that conflict or inconsistency relates to Personal Data.

IN WITNESS WHEREOF, this DPA is entered into and becomes a binding part of the Agreement(s) between Customer and the Regional CA Entity, which is party to the Agreement, as of Customer's Signature Date below. If this document has been electronically signed by either party such signature will have the same legal affect as a hand-written signature.

Agreed for and on behalf of CA	Agreed for and on behalf of Customer
CA Inc., 1320 Ridder Park Drive, San Jose, CA 95131, CA, Inc., 1320 Ridder Park Drive, San Jose, CA 95131 DocuSigned by:  4AF36F177230453...	Customer:
CA Europe Sarl Route de la Longeraie 7, 1110 Morges, Switzerland DocuSigned by:  51B80188F05742E...	Signature:
CA Programas de Computador, Avenida Dr. Chucri Zaidan, 1240 – 27º andar, Golden Tower, CEP 04711-130 - São Paulo-SP, Brazil - CNPJ/MF 08.469.511/0001-69 DocuSigned by:  532DEB4BE5DC428...	Name/Title:
CA (Singapore) Pte Ltd., 1 Yishun Avenue 7, Singapore, 768923 DocuSigned by:  819EC274964049C	Signature Date:

## Annex 1 to the DPA – Details of Processing of Customer Personal Data

This Annex 1 includes certain details of the Processing of Customer's Personal Data as required by Article 28(3) GDPR (or as applicable, equivalent provisions of any other Data Protection Law).

### 1. Customer Data Protection Officer:

### 2. Subject matter and duration of the Processing of Customer Personal Data:

Customer Personal Data is used to provide the Services as set out in the Agreement. The subject matter and duration of the Processing of the Customer Personal Data are set out in the Agreement and this Addendum.

### 3. The nature and purpose of the Processing of Customer Personal Data:

- Collection
- Recording
- Disclosure
- Deletion
- Alteration
- Restriction
- Use

### 4. The Categories of Customer Personal Data to be Processed may include:

(a) Contact details including but not limited to name, job title and level, business email addresses, phone numbers and office addresses;

(b) Email addresses, IP addresses and other network and devices or software identification information;

(c) Online data (e.g. website usage, browsing activities and preferences and other web traffic data);

(d) Log data which may include certain source and destination IP addresses, host name, user-ids, URLs, policy names, email addresses, date and time stamps, data volumes, email activity and content;

(e) Any Personal Data which may be contained within (i) email and web communications (including their attachments) which are sent to or from employee or users of Customer's network, (ii) any Personal Data that may be shared by Customer's employees or users with cloud applications used in Customer's network, and (iii) technical and support requests raised by or on behalf of Customer; and

(f) Any other email and web activity related Personal Data as required for the provision of the Services.





## Data Processing Addendum

### 5. The Categories of Data Subjects (\*) to whom the Customer Personal Data relates:

Customer's employees, representatives, customers, vendors, and/or any other business contacts including senders and recipients of emails, as applicable.

(\*) Complementary description of the categories of Personal Data and Data Subjects for specific services can be found at <https://www.broadcom.com/company/legal/privacy/transparency>.

### 6. Other Personal Data:

### 7. Special Categories of Personal Data (Art. 9 GDPR):

### 8. Sub-processors:

A current list of Sub-processors is maintained at <https://www.broadcom.com/company/legal/privacy/sub-processors>.

## Annex 2 to the DPA – Security of Processing

CA adopts a standards neutral approach in its commitment towards security of processing. The applicability and scope of various standards (and corresponding controls) may differ with respect to the requirements of a specific business unit, service, product or specific engagement. The controls and standards referenced below reflect a “minimum” standard of policies and procedures and are intended to provide a general confirmation of implementation of such standards across applicable products and solutions.

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, CA shall implement the measures outlined in the documentation available under “Information Security” at <https://www.broadcom.com/company/legal/privacy/data-transfers> to ensure an appropriate level of security for the provision of maintenance and support services and/or the provision of software as a service.

## Annex 3A to the DPA – 2021 Model Clauses (for EU/EEA & Swiss Data Exporters)

**The Parties determine and agree that for the purpose of this Annex:**

☒ **Module 2 applies** (Customer is Controller, CA is Processor).

☐ **Module 3 applies** (Customer is Processor, CA is Sub-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) 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.

#### **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.

## Data Processing Addendum

### 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:

MODULE 2		MODULE 3	
(i)	Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;	(i)	Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
(ii)	Clause 8, Clause 8.1(b), 8.9(a), (c), (d) and (e);	(ii)	Clause 8, Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);
(iii)	Clause 9, Clause 9(a), (c), (d) and (e);	(iii)	Clause 9, Clause 9(a), (c), (d) and (e);
(iv)	Clause 12, Clause 12(a), (d) and (f);	(iv)	Clause 12, Clause 12(a), (d) and (f);
(v)	Clause 13;	(v)	Clause 13;
(vi)	Clause 15.1(c), (d) and (e);	(vi)	Clause 15.1(c), (d) and (e);
(vii)	Clause 16(e);	(vii)	Clause 16(e);
(viii)	Clause 18, Clause 18(a) and (b).	(viii)	Clause 18, Clause 18(a) and (b).

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

### Clause 4 – Interpretation

- (a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- (b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- (c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

### Clause 5 – Hierarchy

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

### Clause 6 – Description of the transfer(s)

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

**Clause 7 – Docking clause**

- (a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
- (b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
- (c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

**SECTION II – OBLIGATIONS OF THE PARTIES****Clause 8 – Data protection safeguards**

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

**8.1 Instructions**

MODULE 2	MODULE 3
<ul style="list-style-type: none"> <li>(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.</li> <li>(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.</li> </ul>	<ul style="list-style-type: none"> <li>(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.</li> <li>(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.</li> <li>(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.</li> <li>(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</li> </ul>

## Data Processing Addendum

	legal act under Union or Member State law between the controller and the data exporter.
--	---

### 8.2 Purpose limitation

MODULE 2	MODULE 3
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.	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

MODULE 2	MODULE 3
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 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.	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 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 (Module 2) / controller (Module 3) 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



## Data Processing Addendum

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 (Module 2) / the data exporter of the controller (Module 3). 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.

MODULE 2	MODULE 3
(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.	(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

## Data Processing Addendum

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

MODULE 2	MODULE 3
The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:	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 (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

- (i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
- (iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

### 8.9 Documentation and compliance

MODULE 2	MODULE 3
(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses. h) (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 Parties shall be able to demonstrate compliance with these Clauses. In particular,	(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. j) (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. k) (c) The data importer shall make all information necessary to demonstrate compliance with the

## Data Processing Addendum

<p>the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.</p> <p>i)</p> <p>(d) 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.</p> <p>(e) 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.</p> <p>(f) 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.</p>	<p>obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.</p> <p>l)</p> <p>(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.</p> <p>m)</p> <p>(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.</p> <p>(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.</p> <p>(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.</p>
--	--

## Clause 9 – Use of sub-processors

MODULE 2	MODULE 3
<p>(a) 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 <b>30 days</b> 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.</p> <p>(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it</p>	<p>(a) 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 <b>30 days</b> 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).</p>

## Data Processing Addendum

<p>shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.</p> <p>(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.</p>	<p>(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. 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.</p> <p>(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.</p>
--	---

- (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**

<b>MODULE 2</b>	<b>MODULE 3</b>
<p>(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.</p> <p>(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</p>	<p>(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.</p> <p>(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</p>

## Data Processing Addendum

<p>provided, as well as the scope and the extent of the assistance required.</p> <p>(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.</p>	<p>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.</p> <p>(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.</p>
--	---

### Clause 11 – Redress

- (a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.
- (b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
- (c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
  - (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
  - (ii) refer the dispute to the competent courts within the meaning of Clause 18.
- (d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- (e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- (f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

### Clause 12 – Liability

- (a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- (b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
- (c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

## Data Processing Addendum

- (d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
- (e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- (f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.
- (g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

### **Clause 13 – Supervision**

- (a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.
- (b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

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

### **Clause 14 – Local laws and practices affecting compliance with the Clauses**

- (a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
- (b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
  - (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
  - (ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;



## Data Processing Addendum

- (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.

MODULE 2	MODULE 3
<p>(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).</p> <p>(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.</p>	<p>(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). The data exporter shall forward the notification to the controller.</p> <p>(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, 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 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.</p>

## Data Processing Addendum

### Clause 15 – Obligations of the data importer in case of access by public authorities

#### 15.1 Notification

- (a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
- (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
  - (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

MODULE 2	MODULE 3
[intentionally blank: not applicable]	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.

MODULE 2	MODULE 3
(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.).	(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.). 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

## Data Processing Addendum

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).

MODULE 2	MODULE 3
(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.	(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. 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.

MODULE 2	MODULE 3
In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.	In these cases, it shall inform the competent supervisory authority 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.

## Data Processing Addendum

- |  |  |
|--|--|
|  |  |
|--|--|
- (d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
- (e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

**Clause 17 – Governing law**

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

**Clause 18 – Choice of forum and jurisdiction**

- (a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- (b) The Parties agree that those shall be the courts of **the Netherlands**.
- (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 2021 Model Clauses

### Annex I to the 2021 Model Clauses

#### 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]

1. Name:

Address:

Contact person's name, position and contact details:

Activities relevant to the data transferred under these Clauses: Utilisation of the cloud and/or support services ordered from the Data importers

Signature and date:

Insert DocuSign stamp in frame:

Role (controller/processor): Controller (respectively Processor if Module 3 is selected)

2.

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

1. Name: CA Europe Sarl

Address: Route de la Longeraie 7, 1110 Morges, Switzerland

Contact person's name, position and contact details: Chrystel Cayzac, attorney for CA Europe Sarl, [data.privacy@broadcom.com](mailto:data.privacy@broadcom.com)

Activities relevant to the data transferred under these Clauses: Provision of the cloud and/or support services ordered by the Data exporter(s)

Signature and date: Per execution on Page 7 above

Role (controller/processor): Processor (respectively Sub-Processor if Module 3 is selected)

2. The other CA affiliates listed at <https://www.broadcom.com/company/legal/privacy/sub-processors>

#### B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

As specified in the transparency notices of the CA products and services utilised by the Data exporter(s), as available at <https://www.broadcom.com/company/legal/privacy/transparency>

Categories of personal data transferred

## Data Processing Addendum

As specified in the transparency notices of the CA products and services utilised by the Data exporter(s), as available at <https://www.broadcom.com/company/legal/privacy/transparency>

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.

Not applicable unless otherwise specified in the transparency notices of the CA products and services utilised by the Data exporter(s), as available at <https://www.broadcom.com/company/legal/privacy/transparency>

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

Ongoing basis for cloud products and services, one-off basis for support requests and other bespoke customer submissions

Nature of the processing

Collection, analysis, correlation, reporting and/or storage, as specified in the transparency notices of the CA products and services utilised by the Data exporter(s), as available at <https://www.broadcom.com/company/legal/privacy/transparency>

Purpose(s) of the data transfer and further processing

As specified in the transparency notices of the CA products and services utilised by the Data exporter(s), as available at <https://www.broadcom.com/company/legal/privacy/transparency>

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

As specified in the transparency notices of the CA products and services utilised by the Data exporter(s), as available at <https://www.broadcom.com/company/legal/privacy/transparency>

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

As specified in the transparency notices of the CA products and services utilised by the Data exporter(s), as available at <https://www.broadcom.com/company/legal/privacy/transparency>, and as complemented by the additional sub-processor information available at <https://www.broadcom.com/company/legal/privacy/sub-processors>.

### C. COMPETENT SUPERVISORY AUTHORITY

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

- For matters related to data transfers pursuant to Regulation (EU) 2016/679:

Autoriteit Persoongegevens of the Netherlands: <https://www.autoriteitpersoonsgegevens.nl/en>

- For matters related to data transfers pursuant to, until December 31, 2022, the Swiss Federal Act on Data Protection of 19 June 1992 (SR 235.1; "FADP"), and from January 1, 2023 onwards, the Revised Swiss Federal Act on Data Protection of 25 September 2020 ("Revised FADP"):

Federal Data Protection and Information Commissioner of Switzerland:  
<https://www.edoeb.admin.ch/edoeb/en/home.html>



## Annex II to the 2021 Model Clauses – Technical and Organisational Measures Including Technical and Organisational Measures to Ensure the Security of the Data

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

As described in the documentation available under “Information Security” at <https://www.broadcom.com/company/legal/privacy/data-transfers>

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

CA contractually requires all sub-processors to take technical and organisational measures at least equivalent to, and in any case no less protective than those referenced above.

### Third-Country Addendum to the 2021 Model Clauses: Switzerland

For the purposes of these Clauses, the term 'member state' shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c).

Until December 31, 2022, these Clauses shall also protect the data of legal entities in the scope of the Swiss Federal Act on Data Protection of 19 June 1992 (SR 235.1; "FADP").

## Annex 3B to the DPA – International Data Transfer Addendum (for UK Data Exporters)

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

**VERSION B1.0, in force 21 March 2022**

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

### Part 1: Tables

**Table 1: Parties**

<b>Start date</b>		
<b>The Parties</b>	<b>Exporter (who sends the Restricted Transfer)</b>	<b>Importer (who receives the Restricted Transfer)</b>
<b>Parties' details</b>	Full legal name: <input type="text"/> Trading name (if different): <input type="text"/> Main address (if a company registered address): <input type="text"/> Official registration number (if any) (company number or similar identifier): <input type="text"/>	Full legal name: CA Europe Sarl Trading name (if different): <input type="text"/> Main address (if a company registered address): Route de la Longeraie 7, 1110 Morges, Switzerland Official registration number (if any) (company number or similar identifier): <input type="text"/>
<b>Key Contact</b>	Full Name (optional): <input type="text"/> Job Title: <input type="text"/> Contact details including email: <input type="text"/>	Full Name (optional): Christel Cayzac Job Title: <input type="text"/> Contact details including email: <a href="mailto:data.privacy@broadcom.com">data.privacy@broadcom.com</a>
<b>Signature (if required for the purposes of Section 2)</b>		

## Data Processing Addendum

**Table 2: Selected SCCs, Modules and Selected Clauses**

<b>Addendum EU SCCs</b>		<input checked="" type="checkbox"/> The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: <input type="text"/> Reference (if any): <input type="text"/> Other identifier (if any): <input type="text"/> Or <input type="checkbox"/> the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:				
Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1						
2						
3						
4						

**Table 3: Appendix Information**

“**Appendix Information**” means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties:

Annex 1B: Description of Transfer: As specified in the transparency notices of the CA products and services utilised by the Data exporter(s), as available at

<https://www.broadcom.com/company/legal/privacy/transparency>

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: **As described in the documentation available under “Information Security” at <https://www.broadcom.com/company/legal/privacy/data-transfers>**

## Data Processing Addendum

Annex III: List of Sub processors (Modules 2 and 3 only): The other CA affiliates listed at <https://www.broadcom.com/company/legal/privacy/sub-processors>

**Table 4: Ending this Addendum when the Approved Addendum Changes**

<b>Ending this Addendum when the Approved Addendum changes</b>	Which Parties may end this Addendum as set out in Section 0: <input checked="" type="checkbox"/> Importer <input checked="" type="checkbox"/> Exporter <input type="checkbox"/> neither Party
--	--

### Part 2: Mandatory Clauses

#### Entering into this Addendum

Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

#### Interpretation of this Addendum

Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

<b>Addendum</b>	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
<b>Addendum EU SCCs</b>	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
<b>Appendix Information</b>	As set out in Table 3.
<b>Appropriate Safeguards</b>	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are

## Data Processing Addendum

	making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum 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 0.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.



## Data Processing Addendum

### Hierarchy

Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 0 will prevail.

Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

### Incorporation of and changes to the EU SCCs

This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

- a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;
- b. Sections 0 to 0 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and
- c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

Unless the Parties have agreed alternative amendments which meet the requirements of Section 0, the provisions of Section 0 will apply.

No amendments to the Approved EU SCCs other than to meet the requirements of Section 0 may be made.

The following amendments to the Addendum EU SCCs (for the purpose of Section 0) are made:

- a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;
- b. In Clause 2, delete the words:  
  
"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";
- c. Clause 6 (Description of the transfer(s)) is replaced with:

## Data Processing Addendum

“The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter’s processing when making that transfer.”;

- d. Clause 8.7(i) of Module 1 is replaced with:

“it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer”;

- e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

“the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;”

- f. References to “Regulation (EU) 2016/679”, “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)” and “that Regulation” are all replaced by “UK Data Protection Laws”. References to specific Article(s) of “Regulation (EU) 2016/679” are replaced with the equivalent Article or Section of UK Data Protection Laws;

- g. References to Regulation (EU) 2018/1725 are removed;

- h. References to the “European Union”, “Union”, “EU”, “EU Member State”, “Member State” and “EU or Member State” are all replaced with the “UK”;

- i. The reference to “Clause 12(c)(i)” at Clause 10(b)(i) of Module one, is replaced with “Clause 11(c)(i)”;

- j. Clause 13(a) and Part C of Annex I are not used;

- k. The “competent supervisory authority” and “supervisory authority” are both replaced with the “Information Commissioner”;

- l. In Clause 16(e), subsection (i) is replaced with:

“the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;”;

- m. Clause 17 is replaced with:

“These Clauses are governed by the laws of England and Wales.”;

- n. Clause 18 is replaced with:

“Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts.”; and

## Data Processing Addendum

O. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

### Amendments to this Addendum

The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

From time to time, the ICO may issue a revised Approved Addendum which:

- a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
- b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

If the ICO issues a revised Approved Addendum under Section 0, if any Party selected in Table 4 “Ending the Addendum when the Approved Addendum changes”, will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

- a its direct costs of performing its obligations under the Addendum; and/or
- b its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.