

---

## 1. Operation of this Data Processing Addendum

- (a) This Data Processing Addendum (the **DPA**) is an addendum to each agreement (however constituted, including by multiple documents; in whatever form, including an Order; and as amended from time to time, each an **Agreement**) entered into, or to be entered into, by Catapult and the customer entity (or its Affiliates, as applicable) as identified in the Agreement (the **Customer** or **you**). It amends, changes, and modifies the terms and conditions of the Agreement with effect on and from the DPA Effective Date.
- (b) Capitalized terms used but not defined in this Addendum have the meanings given to them in the Agreement.
- (c) This DPA prevails to the extent of any inconsistency with the Agreement. It contains all the terms agreed between the parties regarding the Processing of Personal Data under the Agreement with respect to the period on and from the DPA Effective Date, and replaces any prior agreement, understanding or arrangement between the parties, whether oral or in writing, relating to the same.
- (d) This DPA is version 20240301.

---

## 2. Definitions

**Affiliate** means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. For the purposes of this definition, "control" means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

**Australian Data Protection Law** means the Australian Privacy Act 1988 (Cth).

**Brazilian Data Protection Law** means the Brazilian General Data Protection Law No. 13,709/2018 (**LGPD**).

**Catapult** means the applicable Catapult Group Company that contracts with you under the Agreement; and its Affiliates that are engaged in the Processing of your Personal Data.

**Catapult Group** means CGIL and its Affiliates.

**Catapult Group Company** means a member of the Catapult Group.

**CGIL** means Catapult Group International Ltd ABN 53 164 301 197.

**Controller** means the entity which determines the purposes and means of the Processing of Personal Data.

**Customer Data** has the same meaning as "Data" under the Agreement.

**Data Protection Laws** means all laws and regulations applicable to the Processing of Personal Data under the Agreement, including Australian Data Protection Law, Brazilian Data Protection Law, European Data Protection Law, and US Data Protection Law.

**Data Subject** means the individual to whom Personal Data relates.

**DPA Effective Date** means, in relation to an Agreement, the later of the date of this DPA, the Term Start Date for that Agreement, and, in relation to an amendment or variation to this DPA, the effective date of any such amendments or variations determined in accordance with clause 12.3(b).

**EU Standard Contractual Clauses** means the binding agreement by and between you and Catapult attached as Schedule 2 to this DPA which contains the standard contractual clauses, including the provisions of "Module Two: Transfer controller to processor", approved by the European Commission's decision 2021/914 of 4 June 2021 for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection under the EU GDPR.

**European Data** means Personal Data that is subject to the protection of European Data Protection Law.

**European Data Protection Law** means (as applicable):

- (a) the 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, and repealing Directive 95/46/EC (**EU GDPR**); or
- (b) the EU GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018, and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2020) (**UK GDPR**).

**Personal Data** means personal data, personal information or personally identifiable information as defined under applicable Data Protection Law.

**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 by Catapult or its Sub-processors. Personal Data Breach does not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

**Processing** means any operation or set of operations that are performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

**Processor** means the entity which Processes Personal Data on behalf of the Controller.

**Standard Contractual Clauses** means the EU Standard Contractual Clauses or the UK Addendum, as applicable.

**Sub-processor** means any Processor engaged by Catapult or by another Sub-processor.

**Supervisory Authority** means an independent public authority which is established by an EU Member State or the UK pursuant to European Data Protection Law.

**UK Addendum** means the binding agreement by and between you and Catapult attached as Schedule 3 which contains the standard contractual clauses, including the EU Standard Contractual Clauses as amended and incorporated into the International Data Transfer Addendum approved by the UK Information Commissioner and adopted by the UK under s119A(1) of the Data Protection Act 2018.

**US Data** means Personal Data that is subject to the protection of US Data Protection Laws.

**US Data Protection Law** refers to the California Consumer Privacy Act of 2018, and any amendments or implementing regulations, including the *California Consumer Privacy Act* (**CCPA**) CAL. CIV. CODE TITLE 1.81.5, § 1798.100 *et seq.* and the *California Privacy Rights Act* (**CPRA**), as well as similar statutes, including Colorado's Privacy Act (**CPA**), COLO. REV. STAT. § 6-1-1301 *et seq.*, Connecticut's Data Privacy Act (**CDPA**), S.B. 6, 2022 Gen. Assemb., Reg. Sess., Utah's Consumer Privacy Act (**UCPA**), S.B. 227, 2022, Gen. Assemb., Reg. Sess., and Virginia Consumer Data Protection Act (**VCDPA**), VA. CODE ANN. §§ 59.1-575 *et seq.*

---

## 3. Roles of the Parties

The parties acknowledge and agree that with regard to the Processing of Personal Data by Catapult on your behalf in connection with Catapult performing its obligations under the Agreement, you are the Controller, Catapult is a Processor and that Catapult may engage Sub-processors in accordance with clause 6.



### 3.1 Your obligations

- (a) You must comply with your obligations in accordance with the requirements of applicable Data Protection Laws, including by providing Data Subjects with all necessary notices and obtaining all necessary consents required for Catapult to process Personal Data for the purposes set out in the Agreement.
- (b) For the avoidance of doubt, your instructions to Catapult for the Processing of Personal Data in connection with the Agreement shall comply with applicable Data Protection Laws. In particular, you acknowledge that you have sole responsibility for (i) the accuracy, quality, and legality of such Personal Data and the means by which you acquired such Personal Data; (ii) complying with all necessary transparency and lawfulness requirements under applicable Data Protection Laws for the collection and use of the Personal Data, including obtaining any necessary consents and authorizations (iii) ensuring you have the right to transfer, or provide access to, the Personal Data to us for Processing in accordance with the terms of the Agreement (including this DPA); (iv) ensuring that your instructions to us regarding the Processing of Personal Data comply with applicable laws, including Data Protection Laws. You will inform us without undue delay if you are not able to comply with your responsibilities under this clause 3 or applicable Data Protection Laws.
- (c) You acknowledge that the Agreement (including this DPA), together with your use of Catapult's Products, Software or Services in accordance with the Agreement, constitutes your complete instructions to us in relation to the Processing of Personal Data, so long as you may provide additional instructions during the Term that are consistent with the Agreement, as well as the nature and lawful use of the Catapult's Products, Software or Services.

### 3.2 Catapult's obligations

- (a) Catapult shall only process Personal Data for the purposes described in this DPA or otherwise agreed within the scope of your lawful written instructions, except where and to the extent otherwise required by applicable law. Catapult is not responsible for compliance with any Data Protection Laws applicable to you that are not generally applicable to us.
- (b) If Catapult becomes aware that it cannot Process Personal Data in accordance with your instructions due to a legal requirement under any applicable law, Catapult will (i) promptly notify you of that legal requirement to the extent permitted by the applicable law; and (ii) where necessary, cease all Processing (other than merely storing and maintaining the security of the affected Personal Data) until such time as you issue new instructions with which Catapult is able to comply. If this provision is invoked, Catapult will not be liable to you under the Agreement for any failure to perform the applicable services until such time as you issue new lawful instructions with regard to the Processing.

---

## 4. Data Subject Requests

- (a) If Catapult receives a request from a Data Subject to exercise the Data Subject's rights (under applicable Data Protection Laws) in respect of the Personal Data processed by Catapult under the Agreement (**Data Subject Request**), Catapult shall, to the extent legally permitted, (i) use commercially reasonable efforts to promptly notify you, and (ii) advise the Data Subject to submit their request to you. You will be solely responsible for responding substantively to any such Data Subject Requests or similar communications involving Personal Data.
- (b) To the extent you are unable to independently address a Data Subject Request, or requests from data protection authorities, relating to the Processing of Personal Data under the Agreement, then upon your written request Catapult will provide reasonable assistance to you to enable you to respond to any such requests.

You will reimburse Catapult for any commercially reasonable costs arising from this assistance.

---

## 5. Confidentiality obligations of Catapult Personnel

Catapult shall ensure that any personnel whom it authorizes to Process Personal Data on its behalf are subject to appropriate confidentiality obligations.

---

## 6. Sub-Processors

### 6.1 Appointment of Sub-processors

- (a) You acknowledge and agree that Catapult may engage Sub-Processors to Process Personal Data on your behalf, including (i) to assist Catapult with hosting and infrastructure, (ii) to support product features and integrations, and (iii) to assist Catapult with service and support.
- (b) Where Catapult engages Sub-Processors, Catapult will impose data protection terms on the Sub-Processors that provide at least the same level of protection for Personal Data as those in this DPA to the extent applicable to the nature of the services provided by such Sub-Processors.

### 6.2 Changes to Sub-processors

Catapult will maintain an up-to-date list of its Sub-processors, including third parties and Catapult Affiliates, and make it available at [catapult.com/standard-terms](https://catapult.com/standard-terms). Catapult will update this list at least 30 days before engaging a new Sub-processor. You may subscribe to receive notifications by email to any changes in Sub-Processors by sending a request to [privacy@catapult.com](mailto:privacy@catapult.com), in which case Catapult will notify you by email at least 30 days prior to any such change.

### 6.3 Objection Right for New Sub-processors

You may object to Catapult's appointment or replacement of a Sub-Processor in writing within 14 days after receipt of Catapult's notice provided in accordance with clause 6.2, provided that such objection is based on reasonable grounds relating to the protection of your Personal Data. In such an event, the parties will discuss your concerns in good faith with a view to achieving a commercially reasonable resolution. If no such resolution can be reached, Catapult will either (i) not appoint; or (ii) replace, the Sub-processor for the purposes of Processing your Personal Data. If Catapult determines at its sole discretion that either option is not reasonably practicable, you may suspend or terminate the affected Product, Software or Services under the Agreement without liability to either party (but without prejudice to any fees incurred by you up to and including the date of suspension or termination). If you do not object during the relevant period, Catapult will deem you to have authorized the appointment or replacement of the Sub-processor, as applicable.

### 6.4 Liability

Catapult is responsible for each Sub-Processor's compliance with the obligations of this DPA and for any acts or omissions of such Sub-Processor that cause Catapult to breach any of its obligations under this DPA.

---

## 7. Data Transfers

You acknowledge and agree that the Catapult Group may access and Process Personal Data on a global basis as necessary to provide the Products, Software or Service in accordance with the Agreement and, in particular, that Personal Data may be transferred to, and Processed by, Catapult Sports Inc. in the United States and to other jurisdictions where Catapult Affiliates and Sub-Processors have operations. Wherever Personal Data is transferred outside its country of origin, each party will ensure such transfers are made in compliance with the requirements of Data Protection Laws.

---

## 8. Security

- (a) Catapult shall maintain appropriate technical and organizational measures to protect Personal Data from Personal Data Breaches,

as set out in Annex 2 to Schedule 2 of this DPA (the **Security Measures**). Notwithstanding any provision to the contrary, Catapult may modify or update the Security Measures at its discretion provided that such modification or update does not result in a material degradation in the protection offered by the Security Measures.

- (b) You are responsible for independently determining whether the data security provided by Catapult in relation to the Agreement adequately meets your obligations under applicable Data Protection Laws. You are also responsible for your secure use of Catapult's Products, Software and Services, including protecting the security of Personal Data in transit to and from the Products Software and Services (including to securely backup or encrypt any such Personal Data).

---

## 9. Personal Data Breach management and notification

- (a) Catapult shall notify you without undue delay after it becomes aware of a Personal Data Breach. Catapult shall take commercially reasonable measures and actions to remedy or mitigate the effects of the Personal Data Breach to the extent remediation is within Catapult's reasonable control, and shall keep you informed of all material developments in connection with the Personal Data Breach.
- (b) At your request, Catapult will promptly provide you with such reasonable assistance as necessary to enable you to notify competent authorities and affected Data Subjects of relevant Personal Data Breaches, if you are required to do so under Data Protection Laws.

---

## 10. Audit, return and deletion of Customer Data

### 10.1 Audit

Catapult shall, to the extent required by applicable Data Protection Laws: (i) make available to you information reasonably necessary to demonstrate Catapult's compliance with this DPA; and (ii) permit you (or an independent third party acting on your behalf), on one occasion in any 12-month period only, to perform an audit strictly limited to Catapult's arrangements for complying with this DPA, provided that such audit is carried out during Catapult's normal business hours and that you (or the relevant third party conducting such an audit) gives Catapult a reasonable period of notice before carrying out the audit.

### 10.2 Return and deletion of Customer Data

- (a) At any time up to the expiration or termination of the Agreement, and for 90 days following the termination date (or such later date as prescribed by applicable Data Protection Laws) and subject to the terms of the Agreement, you may request the return or deletion of Customer Data by sending a request to [privacy@catapult.com](mailto:privacy@catapult.com).
- (b) Following termination or expiration of the Agreement, Catapult shall delete all Customer Data, including Personal Data Processed pursuant to this DPA, except (i) where Catapult is required by applicable law or its internal data retention policies to retain some or all Customer Data, (ii) to the extent Catapult is permitted to retain such Customer Data under the Agreement; and (iii) where Catapult has archived Customer Data on back-up systems, in which circumstances such data will be securely isolated, protected from any further Processing and deleted in accordance with Catapult's deletion practices.
- (c) Catapult strongly recommends retrieving your Customer Data prior to the end of the Agreement. If you need help retrieving your Customer Data, Catapult will provide reasonable assistance to you, at your cost, and in accordance with the 'Confidentiality' section of Catapult's standard terms and conditions as incorporated in the Agreement.

---

## 11. Additional Provisions for European Data

### 11.1 Scope

This clause 11 applies only with respect to your Customer Data which is "European Data".

### 11.2 Roles of the Parties

When Processing European Data in accordance with your instructions, the parties acknowledge and agree that you are the Controller of European Data and Catapult is the Processor.

### 11.3 Instructions

If Catapult believes that your instruction infringes European Data Protection Law (where applicable), Catapult will inform you without undue delay.

### 11.4 Sub-Processor Agreements

For the purposes of clause 9(c) of the Standard Contractual Clauses, you acknowledge that Catapult may be restricted from disclosing Sub-Processor agreements, but Catapult will use reasonable efforts to require any Sub-Processor that Catapult appoints to permit Catapult to disclose the Sub-Processor agreement to you and Catapult will provide (on a confidential basis) all information it reasonably can.

### 11.5 Data Protection Impact Assessment

Upon your request, Catapult shall provide you with reasonable cooperation and assistance to fulfil your obligation under European Data Protection Law to carry out a data protection impact assessment related to your use of the Products, Software or Services, to the extent (i) you do not otherwise have access to the relevant information, and (ii) such information is available to Catapult. Upon request, Catapult shall also provide reasonable assistance to you in any prior consultation with a relevant Supervisory Authority (in the performance of its tasks relating to this clause 11.5) to the extent required under European Data Protection Law.

### 11.6 Transfer Mechanisms for Data Transfers

- (a) Catapult will not transfer European Data to any country or recipient not recognized as providing an adequate level of protection for Personal Data (within the meaning of applicable European Data Protection Laws), unless it first takes all such measures as are reasonably necessary to ensure the transfer is in compliance with applicable European Data Protection Laws. Such measures may include transferring such data (i) to a recipient that is covered by a suitable framework or other legally adequate transfer mechanism recognized by the relevant authorities or courts as providing an adequate level of protection for Personal Data (ii) to a recipient that has achieved binding corporate rules authorization in accordance with European Data Protection Laws, or (iii) to a recipient that has executed appropriate standard contractual clauses in each case as adopted or approved in accordance with applicable European Data Protection Laws.
- (b) Subject to clause 11.6(c), in respect of any European Data processed by Catapult on your behalf under this DPA, the parties agree that the Standard Contractual Clauses will be incorporated by reference and form part of the Agreement as follows:
  - (i) **EEA Transfers** – in relation to European Data that is subject to the EU GDPR, (A) Customer is the "data exporter" and Catapult is the "data importer"; (B) the Module Two terms apply to the extent the Customer is a Controller of European Data (C) in Clause 7, the optional docking clause does not apply; (D) in Clause 9, Option 2 applies and changes to Sub-Processors will be notified in accordance with clause 6 of this DPA; (E) in Clause 11, the optional language is deleted; (F) in Clauses 17 and 18, the parties agree that the governing law and forum for disputes for the Standard Contractual Clauses will be the Republic of Ireland; (G) the Annexes of the Standard Contractual Clauses will be



deemed completed with the information set out in the Annexes of this DPA; and (H) if and to the extent the Standard Contractual Clauses conflict with any provision of this DPA, the Standard Contractual Clauses will prevail to the extent of such conflict.

- (ii) **UK Transfers** – in relation to European Data that is subject to the UK GDPR, the Standard Contractual Clauses will apply in accordance with clause 11.6(b)(i) and the following modifications: (A) the Standard Contractual Clauses will be modified and interpreted in accordance with the UK Addendum, which will be incorporated by reference and form an integral part of the Agreement; (B) Tables 1, 2 and 3 of the UK Addendum will be deemed completed with the information set out in the Annexes of this DPA and Table 4 will be deemed completed by selecting “neither party”; and (C) any conflict between the terms of the Standard Contractual Clauses and the UK Addendum will be resolved in accordance with sections 10 and 11 of the UK Addendum.
- (c) If Catapult cannot comply with its obligations under the Standard Contractual Clauses or is in breach of any warranties under the Standard Contractual Clauses or UK Addendum (as applicable) for any reason, and you intend to suspend the transfer of European Data to Catapult or terminate the Standard Contractual Clauses, or UK Addendum, you agree to provide Catapult with reasonable notice to enable Catapult to cure such non-compliance and reasonably cooperate with Catapult to identify what additional safeguards, if any, may be implemented to remedy such non-compliance. If Catapult has not or cannot cure the non-compliance, you may suspend or terminate the affected part of the Products, Software or Service in accordance with the Agreement without liability (but without prejudice to any fees you have incurred prior to such suspension or termination).

notice in writing to you, terminate the Agreement, in which case Catapult shall refund you any pre-paid fees for the terminated Products, Software or Services less a pro rata portion for services rendered prior to the date of termination.

---

## 12. General Provisions

### 12.1 Governing Law

This DPA will be governed by and construed in accordance with the governing law and jurisdiction provisions in the Agreement, unless otherwise required by applicable Data Protection Law.

### 12.2 Limitation of liability

Notwithstanding anything to the contrary in the Agreement or this DPA and to the extent permitted by law, the liability of each party and each party's Affiliates under this DPA is subject to the exclusions and limitations set out in the Agreement.

### 12.3 Changes to this DPA

- (a) This clause 12.3 applies to all changes to this DPA other than those addressed by clauses 6.2 and 6.3.
- (b) Catapult may modify some or all of this DPA by posting a revised version of this DPA at [catapult.com/standard-terms](https://catapult.com/standard-terms). The revised DPA will take effect on and from the effective date specified by Catapult therein (the **Effective Date**). The Effective Date must be at least 14 calendar days after the date it is posted on the above website. If the proposed modification is materially adverse to you then (i) Catapult shall notify you in writing of the proposed modification; (ii) the Effective Date for that modification must be at least 14 calendar days after the date you are notified of such proposed modification; (iii) if you disagree with the proposed modification then you may notify Catapult of the same within that 14 calendar day period; (iv) if you validly give such notice within that period then the Agreement (excluding the proposed modification) will continue to apply until the earlier of your next renewal date or the end of the term, after which time the then current terms of this DPA will apply; and (v) if Catapult (acting reasonably) considers that it cannot provide the Products, Software or Services to you under the terms of this DPA (excluding the proposed modifications) then Catapult may, by



## Schedule 1 – Details of the Processing

---

### 1. Categories of Data Subjects whose Personal Data is Transferred

You may submit Personal Data in the course of using the Products, Software or Services. The extent to which you submit such data is determined and controlled by you in your sole discretion. Such Personal Data may include Personal Data relating to the following categories of Data Subjects:

- (a) athletes whose personal data is collected using the relevant Catapult Products, Software or Services; and
- (b) your Personnel and other end users who access and use the Products, Software or Services.

---

### 2. Categories of Personal Data Transferred

You may submit Personal Data in the course of using the Products, Software or Services. The extent to which you submit such data is determined and controlled by you in your sole discretion. Such data may include the following categories of Personal Data:

- (a) in respect of the Products and Software: first name, last name, date of birth (optional), height, weight, image, playing position, team, positional data (GPS or LPS), inertial data (accelerometers, gyroscopes, magnetometer), and heart rate data (depending on specific Product and subscription type);
- (b) in respect of the Services: username and email, phone number (optional for multi-factor authentication); and
- (c) any other Personal Data submitted by, sent to, or received by you, or your end users, via the Products, Software or Services.

---

### 3. Sensitive Data transferred and applied restrictions or safeguards

You may submit sensitive data in the course of using the Products, Software or Services. The extent to which you submit such sensitive data is determined and controlled by you in your sole discretion. Such sensitive data may include heart rate data (depending on specific Product and subscription type).

Restrictions and safeguards applied in the protection of sensitive data include data encryption as detailed in Annex 2.

---

### 4. Frequency of the transfer

Continuous.

---

### 5. Nature of the Processing

Personal Data will be Processed in accordance with the Agreement (including this DPA), and may be subject to the following Processing activities:

- (a) storage and other Processing necessary to provide, maintain and improve the Products, Software or Services provided to you; and/or
- (b) disclosure in accordance with the Agreement (including this DPA) and/or as compelled by applicable laws.

---

### 6. Purpose of the transfer and further processing

Catapult will Process Personal Data as necessary to provide the Products, Software and Services in accordance with the Agreement, or as further instructed by you in your use of the Products, Software or Services.

---

### 7. Period for which Personal Data will be retained

Subject to clause 10.2 of this DPA, Catapult will Process Personal Data for the duration of the Agreement, unless otherwise agreed in writing.



# CATAPULT

Schedule 2 – EU Standard Contractual Clauses

---



Brussels, 4.6.2021  
C(2021) 3972 final

ANNEX

**ANNEX**

*to the*

**COMMISSION IMPLEMENTING DECISION**

**on standard contractual clauses for the transfer of personal data to third countries  
pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council**

## ANNEX

### STANDARD CONTRACTUAL CLAUSES

#### SECTION I

##### *Clause 1*

##### ***Purpose and scope***

- (a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)<sup>1</sup> 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

---

<sup>1</sup> 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 [...].



select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

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

### *Clause 3*

#### ***Third-party beneficiaries***

- (a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
  - (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
  - (ii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);
  - (iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
  - (iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);
  - (v) Clause 13;
  - (vi) Clause 15.1(c), (d) and (e);
  - (vii) Clause 16(e);
  - (viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.
- (b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

### *Clause 4*

#### ***Interpretation***

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

*Clause 5*

***Hierarchy***

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

*Clause 6*

***Description of the transfer(s)***

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

*Clause 7 - 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 ONE: Transfer controller to controller**

**8.1 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. It may only process the personal data for another purpose:

- (i) where it has obtained the data subject's prior consent;
- (ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

## **8.2 Transparency**

- (a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:
  - (i) of its identity and contact details;
  - (ii) of the categories of personal data processed;
  - (iii) of the right to obtain a copy of these Clauses;
  - (iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.
- (b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.
- (c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties 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.
- (d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

## **8.3 Accuracy and data minimisation**

- (a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.
- (b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.
- (c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

## **8.4 Storage limitation**

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures

to ensure compliance with this obligation, including erasure or anonymisation<sup>2</sup> of the data and all back-ups at the end of the retention period.

## **8.5 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 personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter “personal data breach”). In assessing 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.
- (b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
- (c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- (d) 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 personal data breach, including measures to mitigate its possible adverse effects.
- (e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.
- (f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

---

<sup>2</sup> This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.

- (g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

## **8.6 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 or offences (hereinafter "sensitive data"), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

## **8.7 Onward transfers**

The data importer shall not disclose the personal data to a third party located outside the European Union<sup>3</sup> (in the same country as the data importer or in another third country, hereinafter "onward transfer") unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

- (i) it 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 with respect to the processing in question;
- (iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;
- (iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;
- (v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or
- (vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

---

<sup>3</sup> 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.

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

#### **8.8 Processing under the authority of the data importer**

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

#### **8.9 Documentation and compliance**

- (a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.
- (b) The data importer shall make such documentation available to the competent supervisory authority on request.

### **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<sup>4</sup> (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.

---

<sup>4</sup> 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.



## **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<sup>5</sup>.

---

<sup>5</sup> 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.

## **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 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<sup>6</sup>

---

<sup>6</sup> 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

(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 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.

---

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 purposes of these Clauses.

## **MODULE FOUR: Transfer processor to controller**

### **8.1 Instructions**

- (a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.
- (b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.
- (c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.
- (d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

### **8.2 Security of processing**

- (a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter “personal data breach”). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data<sup>7</sup>, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.
- (b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.
- (c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

### **8.3 Documentation and compliance**

- (a) The Parties shall be able to demonstrate compliance with these Clauses.

---

<sup>7</sup> This includes whether the transfer and further processing 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 or offences.

- (b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

### *Clause 9*

#### *Use of sub-processors*

#### **MODULE TWO: Transfer controller to processor**

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

**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 [*Specify time period*] 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.<sup>8</sup> 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

---

<sup>8</sup> This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

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 1: SPECIFIC PRIOR AUTHORISATION** The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the prior specific written authorisation of the controller. The data importer shall submit the request for specific authorisation at least [*Specify time period*] prior to the engagement of the sub-processor, together with the information necessary to enable the controller to decide on the authorisation. It shall inform the data exporter of such engagement. The list of sub-processors already authorised by the controller can be found in Annex III. The Parties shall keep Annex III up to date.

**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 [*Specify time period*] 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.<sup>9</sup> 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 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

---

<sup>9</sup> This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

sub-processor contract and to instruct the sub-processor to erase or return the personal data.

#### *Clause 10*

#### ***Data subject rights***

### **MODULE ONE: Transfer controller to controller**

- (a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request.<sup>10</sup> The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.
- (b) In particular, upon request by the data subject the data importer shall, free of charge :
- (i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);
  - (ii) rectify inaccurate or incomplete data concerning the data subject;
  - (iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.
- (c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.
- (d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter “automated decision”), which would produce legal effects concerning the data subject or similarly significantly affect him / her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject’s rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

---

<sup>10</sup> That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.



- (i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and
  - (ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.
- (e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.
- (f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.
- (g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

#### **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.

#### **MODULE FOUR: Transfer processor to controller**

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

##### *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.

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body<sup>11</sup> at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

#### **MODULE ONE: Transfer controller to controller**

#### **MODULE TWO: Transfer controller to processor**

#### **MODULE THREE: Transfer processor to processor**

- (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.

---

<sup>11</sup> The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

- (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*

**MODULE ONE: Transfer controller to controller**

**MODULE FOUR: Transfer processor to controller**

- (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) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party 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 under Regulation (EU) 2016/679.
- (c) 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.
- (d) The Parties agree that if one Party is held liable under paragraph (c), 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.
- (e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own 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 ONE: Transfer controller to controller**

#### **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 ONE: Transfer controller to controller**

**MODULE TWO: Transfer controller to processor**

**MODULE THREE: Transfer processor to processor**

**MODULE FOUR: Transfer processor to controller** (*where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU*)

- (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<sup>12</sup>;

---

<sup>12</sup> 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

- (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 ONE: Transfer controller to controller**

#### **MODULE TWO: Transfer controller to processor**

---

other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

## **MODULE THREE: Transfer processor to processor**

**MODULE FOUR: Transfer processor to controller** (*where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU*)

### **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.

[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 ONE: Transfer controller to controller**

###### **MODULE TWO: Transfer controller to processor**

###### **MODULE THREE: Transfer processor to processor**

[OPTION 1: 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 \_\_\_\_\_ (*specify Member State*).]

[OPTION 2 (for Modules Two and Three): These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of \_\_\_\_\_ (*specify Member State*).]

###### **MODULE FOUR: Transfer processor to controller**

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of \_\_\_\_\_ (*specify country*).

#### *Clause 18*

##### *Choice of forum and jurisdiction*

###### **MODULE ONE: Transfer controller to controller**

###### **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 \_\_\_\_\_ (*specify Member State*).

- (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.

#### **MODULE FOUR: Transfer processor to controller**

Any dispute arising from these Clauses shall be resolved by the courts of \_\_\_\_\_ (*specify country*).

## APPENDIX

### 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 be achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

### ANNEX I

#### A. LIST OF PARTIES

**MODULE ONE: Transfer controller to controller**

**MODULE TWO: Transfer controller to processor**

**MODULE THREE: Transfer processor to processor**

**MODULE FOUR: Transfer processor to controller**

**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: ...

Signature and date: ...

Role (controller/processor): ...

2. ...

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

1. Name: ...

Address: ...

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

Activities relevant to the data transferred under these Clauses: ...

Signature and date: ...

Role (controller/processor): ...

2. ...

## **B. DESCRIPTION OF TRANSFER**

**MODULE ONE: Transfer controller to controller**

**MODULE TWO: Transfer controller to processor**

**MODULE THREE: Transfer processor to processor**

**MODULE FOUR: Transfer processor to controller**

*Categories of data subjects whose personal data is transferred*

.....

*Categories of personal data transferred*

.....

*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).*

.....

*Nature of the processing*

.....

*Purpose(s) of the data transfer and further processing*

.....

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

.....

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

.....

**C. COMPETENT SUPERVISORY AUTHORITY**

**MODULE ONE: Transfer controller to controller**

**MODULE TWO: Transfer controller to processor**

**MODULE THREE: Transfer processor to processor**

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

.....

## **ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

**MODULE ONE: Transfer controller to controller**

**MODULE TWO: Transfer controller to processor**

**MODULE THREE: Transfer processor to processor**

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.

*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.*

*[Examples of possible measures:*

*Measures of pseudonymisation and encryption of personal data*

*Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services*

*Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident*

*Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing*

*Measures for user identification and authorisation*

*Measures for the protection of data during transmission*

*Measures for the protection of data during storage*

*Measures for ensuring physical security of locations at which personal data are processed*

*Measures for ensuring events logging*

*Measures for ensuring system configuration, including default configuration*

*Measures for internal IT and IT security governance and management*

*Measures for certification/assurance of processes and products*

*Measures for ensuring data minimisation*

*Measures for ensuring data quality*

*Measures for ensuring limited data retention*

*Measures for ensuring accountability*

*Measures for allowing data portability and ensuring erasure]*

*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*

## **ANNEX III – LIST OF SUB-PROCESSORS**

**MODULE TWO: Transfer controller to processor**

**MODULE THREE: Transfer processor to processor**

EXPLANATORY NOTE:

This Annex must be completed for Modules Two and Three, in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

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

1. Name: ...

Address: ...

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


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

2. ...



## Annex 1 to the Standard Contractual Clauses

### 1A. List of Parties

	Data Exporter	Data Importer
<b>Name:</b>	The Customer, as set out in the Order Form	The Catapult Group Company, as set out in the Order Form
<b>Address:</b>	The Customer's address, as set out in the Order Form	The Catapult Group Company's address, as set out in the Order Form
<b>Contact details:</b>	The Customer's contact details, as set out in the Order Form	Data Protection Officer <a href="mailto:dpo@catapult.com">dpo@catapult.com</a>
<b>Activities relevant to the data transferred under these clauses:</b>	See Annex 1(B) below	See Annex 1(B) below
<b>Signature and date:</b>		DocuSigned by:  <small>2E8CA17864E4470...</small> <b>Will Lopes, Managing Director and CEO</b> Catapult Group International Ltd
<b>Date:</b>		
<b>Role (controller/processor):</b>	Controller	Processor

### 1B. Description of the Transfer

<b>Categories of data subjects whose personal data is transferred</b>	See Schedule 1 of this DPA
<b>Categories of personal data transferred</b>	See Schedule 1 of this DPA
<b>Sensitive data transferred (if applicable)</b>	See Schedule 1 of this DPA
<b>(For sensitive data only: 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.)</b>	See Schedule 1 of this DPA
<b>The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).</b>	See Schedule 1 of this DPA
<b>Nature of the processing</b>	See Schedule 1 of this DPA
<b>Purpose(s) of the data transfer and further processing</b>	See Schedule 1 of this DPA
<b>The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period</b>	See Schedule 1 of this DPA
<b>For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing</b>	See Schedule 1 of this DPA

### 1.C Competent Supervisory Authority

For the purposes of this DPA, the supervisory authority that will act as competent supervisory authority will be the authority located in the Customer's home country (in accordance with clause 1A of this Annex 1).



## Annex 2 to the Standard Contractual Clauses – Security Measures

---

### 1. General Controls

For the purposes of clause 8 of the DPA, Catapult shall implement, or be responsible for its Sub-processor's implementation of, measures designed to:

- (a) deny unauthorised persons access to data-processing equipment used for processing your Personal Data (equipment access control);
  - (a) prevent the unauthorised reading, copying, modification or removal of data media containing your Personal Data (data media control);
  - (b) prevent the unauthorised input of your Personal Data and the unauthorised inspection, modification or deletion of stored Personal Data (storage control);
  - (c) prevent the use of automated data-processing systems by unauthorised persons using data communication equipment used to process your Personal Data (user control);
  - (d) ensure that persons authorised to use an automated data-processing system only have access to your Personal Data covered by their access authorisation (data access control);
  - (e) ensure that it is possible to verify and establish to which individuals your Personal Data has been or may be transmitted or made available using data communication equipment (communication control);
  - (f) ensure that it is subsequently possible to verify and establish which of your Personal Data has been put into automated data-processing systems and when and by whom the input was made (input control);
  - (g) prevent the unauthorised reading, copying, modification or deletion of your Personal Data during transfers of those data or during transportation of data media (transport control);
  - (h) ensure that installed systems used to process your Personal Data may, in case of interruption, be restored (recovery); and
  - (i) ensure that the functions of the system used to process your Personal Data perform, that the appearance of faults in the functions is reported (reliability) and to prevent your stored Personal Data from corruption by means of a malfunctioning of the system (integrity).
- 

### 2. Personnel

For the purposes of clause 8 of the DPA, Catapult shall take reasonable steps to ensure that no person shall be appointed by Catapult to process your Personal Data unless that person:

- (a) is competent and qualified to perform the specific tasks assigned to them by Catapult;
  - (b) has been authorised by Catapult; and
  - (c) has been instructed by Catapult in the requirements relevant to the performance of the obligations of Catapult under the Standard Contractual Clauses, in particular the limited purpose of the Processing.
- 

### 3. Security Controls

The Products, Software or Services include a variety of configurable security controls that allow you to tailor the security of the Products, Software or Service for your own use. For the purposes of clause 8 of the DPA, these controls may include:

- (a) unique user identifiers (**User IDs**) to ensure that activities can be attributed to the responsible individual;
  - (b) the ability to specify the lockout time period;
  - (c) controls on the number of invalid login requests before locking out a User;
  - (d) controls to ensure generated initial passwords must be reset on first use;
  - (e) controls to terminate a User session after a period of inactivity;
  - (f) password length controls;
  - (g) password complexity requirements (requires letters and numbers);
  - (h) verification question before resetting password;
  - (i) the ability to accept logins to the Software from only certain IP address ranges; and
  - (j) the ability to restrict logins to the Software to specific time periods (Developer Edition, Enterprise Edition, and Unlimited Edition only).
- 

### 4. Security Procedures, Policies and Logging

For the purposes of clause 8 of the DPA, the Products, Software or Services are operated in accordance with the following procedures to enhance security:

- (a) user passwords are stored using a one-way hashing algorithm (SHA-256) and are not transmitted in an unencrypted form;
- (b) user access log entries are maintained, which may include records such as date, time, User ID, URL executed or entity ID operated on, operation performed (viewed, edited, etc.) and source IP address (note that source IP address availability is dependent on factors including whether you or your ISP use NAT (Network Address Translation) or PAT (Port Address Translation));
- (c) access logs are kept for a minimum of 90 days;
- (d) access logs are kept in a secure area to prevent tampering;
- (e) your passwords are not recorded in any access logs;
- (f) certain administrative changes to the Products, Software or Services (such as password changes and adding custom fields) are tracked in an area known as the "Setup Audit Log" and are available for viewing by your system administrator (you may download and store this data locally); and
- (g) Catapult does not set a defined password for a user. Passwords are set to a random value (which must be changed on first use) and delivered automatically via email to the requesting user.



---

## 5. Intrusion Detection

For the purposes of clause 8 of the DPA, Catapult, or an authorised third party monitor the Products, Software or Services, as appropriate, for unauthorised intrusions using network-based intrusion detection mechanisms.

---

## 6. User Authentication

For the purposes of clause 8 of the DPA, access to the Products, Software or Services requires, as appropriate, a valid User ID and password combination, which are encrypted via SSL while in transmission. Following a successful authentication, a random session ID is generated, as appropriate, and stored in the user's browser to preserve and track session state.

---

## 7. Security Logs

For the purposes of clause 8 of the DPA, all Catapult or Sub-processor systems used to store Customer Data, including firewalls, routers, network switches and operating systems, log information to their respective system log facility or a centralised syslog server (for network systems).

---

## 8. Incident Management

For the purposes of clause 8 of the DPA, Catapult maintains security incident management policies and procedures.

---

## 9. Physical Security

For the purposes of clause 8 of the DPA, Catapult and its Sub-processors maintain appropriate physical safeguards and control devices designed to prevent unauthorized physical access, damage, and interference..

---

## 10. Reliability and Backup

For the purposes of clause 8 of the DPA, all networking components, SSL accelerators, load balancers, web servers and application servers that are part of the Force.com platform are configured in a redundant configuration. All Personal Data is stored on a primary database server that is clustered with a backup database server for redundancy. All Personal Data is stored on carrier-class disk storage using RAID disks and multiple data paths. All Personal Data, up to the last committed transaction, is automatically backed up on a regular basis. Any backup tapes are verified for integrity stored in an offsite facility in a secure, fire-resistant location.

---

## 11. Disaster Recovery

For the purposes of clause 8 of the DPA, systems in which Customer Data is stored have a disaster recovery facility that is geographically remote from its primary data centre, along with required hardware, software, and Internet connectivity, in the event production facilities at the primary data centre were to be rendered unavailable. Catapult will ensure that its Sub-processors that store Customer Data have disaster recovery plans in place and test them at least once per year.

---

## 12. Viruses

For the purposes of clause 8 of the DPA, the Products, Software or Services will not introduce any viruses to your systems; however, the Products, Software or Services do not scan for viruses that could be included in attachments or other Personal Data uploaded into the Products, Software or Services by you. Any such uploaded attachments will not be executed in the Products, Software or Services and therefore will not damage or compromise the Service.

---

## 13. Data Encryption

For the purposes of clause 8 of the DPA, the Products, Software or Services use industry-accepted encryption products to protect Customer Data and communications during transmissions between a customer's network and the Products, Software or Services, including by 128-bit TLS Certificates and 2048-bit RSA public keys. Additionally, Customer Data is encrypted during transmission between data centres for replication purposes.

---

## 14. System Changes and Enhancements

Catapult's security controls, procedures, policies and features may be changed during the term of the Agreement. Catapult will provide security controls that deliver a level of security protection at least as good as that provided as of the date of the Agreement.



# CATAPULT

**Schedule 3 – International Data Transfer Addendum to the EU Commission Standard Contractual Clauses  
(‘UK Addendum’)**



Information Commissioner's Office

## Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

### 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**

Start date		
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' details	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: <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"/>

<b>Key Contact</b>	Full Name (optional): [REDACTED] Job Title: [REDACTED] Contact details including email: [REDACTED]	Full Name (optional): [REDACTED] Job Title: [REDACTED] Contact details including email: [REDACTED]
<b>Signature (if required for the purposes of Section 2)</b>		

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

<b>Addendum EU SCCs</b>	<input type="checkbox"/> The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: [REDACTED] Reference (if any): [REDACTED] Other identifier (if any): [REDACTED] 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:

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:

Annex III: List of Sub processors (Modules 2 and 3 only):

### 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 19: <input type="checkbox"/> Importer <input type="checkbox"/> Exporter <input type="checkbox"/> neither Party
----------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## Part 2: Mandatory Clauses

### Entering into this Addendum

1. 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.
2. 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

3. 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:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are 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 18.
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.

4. 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.
5. 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.
6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.
7. 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.
8. 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.

### Hierarchy

9. 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 10 will prevail.
10. 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.
11. 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**

12. 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 9 to 11 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.
13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.
14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.
15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) 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:

"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
- 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

16. 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.
17. 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.
18. 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.

19. If the ICO issues a revised Approved Addendum under Section 18, 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.

20. 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.

## Alternative Part 2 Mandatory Clauses:

<b>Mandatory Clauses</b>	Part 2: 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.
--------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------