EXHIBIT E

DATA PROCESSING ADDENDUM

This Data Processing Addendum, including its Schedules and Appendices ("**DPA**") forms part of the ASA ("**Agreement**") or other written or electronic agreement between Ativion and Customer. By signing the Agreement, Customer enters into this DPA on behalf of itself and its Authorized Affiliates. For the purposes of this DPA only, and except where indicated otherwise, the term "**Customer**" shall include Customer and Authorized Affiliates.

All capitalized terms not defined in the DPA shall have the same meaning as those defined in the Agreement, including any Schedules or Appendices. In the course of providing the Services to Customer pursuant to the DPA, Ativion may Process Personal Data on behalf of Customer and the parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith. This DPA supplements the data privacy and security obligations of each Party.

1. DEFINITIONS

"Authorized Affiliate" means any of Customer's Affiliate(s) which (a) is subject to the Data Protection Laws and Regulations, and (b) is permitted to use the Services pursuant to the Agreement between Customer and Ativion, but has not signed its own Order with Ativion and is not a "Customer" as defined under this DPA.

"CCPA" means shall have the same meaning as defined by the Agreement .

"Data Protection Laws and Regulations" shall have the same meaning as defined by the Agreement.

"Data Subject" means the identified or identifiable person to whom Personal Data relates.

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

"Processor" means the legal person which Processes Personal Data on behalf of the Controller, or as the term is defined in the applicable Data Protection Laws and Regulations.

"Security Incident" means the actual unauthorized disclosure, acquisition of, or access to, the Personal Data that does or may compromise the security, confidentiality and/or integrity of the Personal Data.

“Sub-processor” means any Processor engaged by Ativion or a member of the Ativion Group.

The terms **“Business”**, **“Personal Information”**, **“Sell”**, **“Share”**, and **“Service Provider”** shall have the same meaning as the terms defined in the CCPA.

2. PROCESSING OF PERSONAL DATA

2.1. Roles of the Parties. The parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Controller and Business and Ativion is the Processor and Service Provider, as such terms are defined in the applicable Data Protection Laws and Regulations. Ativion will treat the Personal Information as the Confidential Information of Client. Ativion or members of Ativion Group will engage Sub-processors pursuant to the requirements set forth in Section 5 “Sub-processors” below.

2.2. Customer’s Processing of Personal Data. Customer shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations, including any applicable requirement to provide notice to Data Subjects of the use of Ativion as Processor and obtaining consents. For the avoidance of doubt, Customer’s instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.

2.3. Details of the Processing. The subject matter, duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are specified in Exhibit D (Details of the Processing) to this DPA.

2.4. General Provisions. As a Processor Customer’s Personal Data, Ativion shall:

(a) process Personal Data only on Customer’s written instructions (provided that such instructions are within the scope of the Services set out in the Agreement) unless Ativion is required by applicable Data Protections Laws and Regulations to process Personal Data. When such applicable Data Protections Laws and Regulations require processing of Personal Data outside of the scope of Customer’s instructions, Ativion will promptly notify the Customer of this before performing the processing required by the applicable laws unless those applicable laws prohibit Ativion from doing so.

(b) ensure that it has in place appropriate technical and organizational measures to protect against unauthorized or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data, appropriate to the harm that might result from the unauthorized or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures (those measures may include, where appropriate, pseudonymizing and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of its systems and services, ensuring that availability of

and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the technical and organizational measures adopted by it).

(c) ensure that all Ativion personnel who have access to and/or process Personal Data are subject to the duty of confidentiality, contractually or statutorily, to keep the Personal Data confidential.

(d) not transfer any Personal Data outside of the applicable geographic area without ensuring adequate measures are in place to protect the Personal Data as required by applicable Data Protection Laws and Regulation.

(e) reasonably assist Customer in ensuring compliance with the obligations under the Data Protection Laws and Regulations, as applicable, considering the nature of Processing and the information available to Ativion, upon Customer's reasonable request.

(f) maintain records of processing categories of activities carried out on behalf of the Customer.

(g) notify Customer if Ativion believes any Processing required under the Agreement is contrary to Customer's instructions or what is allowed under the applicable Data Protection Laws and Regulations.

(h) notify Customer if Ativion determines that it can no longer meet its obligations under applicable Data Protection Laws and Regulations.

3. DATA SUBJECT REQUEST.

Ativion shall, to the extent legally permitted, promptly notify Customer if Ativion receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure, data portability, object to the Processing, or its right not to be subject to an automated individual decision making, each such request being a "**Data Subject Request**". Taking into account the nature of the Processing, Ativion shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent Customer does not have the ability to address a Data Subject Request, Ativion shall, upon Customer's request, provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent Ativion is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. Customer shall be responsible for any costs arising from Ativion's provision of such assistance.

4. ATIVION PERSONNEL

4.1. Training and Confidentiality. Ativion shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate recurring training on their responsibilities and have executed

written confidentiality agreements. Ativion shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

4.3. Limitation of Access. Ativion shall ensure that access to Personal Data is determined on a principle of least privilege and limited to those personnel performing Services in accordance with the Agreement.

4.4. Data Protection Officer. The Ativion Group has appointed a data protection officer. The data protection officer can be contacted on dpo@ativion.com.

5. SUB-PROCESSORS

5.1. Appointment of Sub-processors. Customer acknowledges and agrees that it provides general authorization to Ativion to engage Sub-processors. Specifically, Customer acknowledges that (a) Ativion's Affiliates may be retained as Sub-processors; and (b) Ativion Group may engage third-party Sub-processors in connection with the provision of the Services. When engaging a Sub-processor, Ativion Group will enter into a written agreement with each Sub-processor containing data protection obligations not less protective than those in this DPA to the extent applicable to the nature of the Services provided by such Sub-processor, including that the Sub-processor will provide sufficient guarantees to implement appropriate technical and organizational measures in such a way that the processing will meet the requirements of applicable Data Protection Laws and Regulations.

5.2. List of Current Sub-processors. Ativion shall make available to Customer, on Ativion's website, the current list of Sub-processors used, and their country of location. The current list of Ativion Sub-processors may be found at: www.ativion.com/legal/sub-processor.

5.3. Objection. Before engaging a new Sub-processor, Ativion will notify Customer with details of the new Sub-processor through an update to its website at www.ativion.com/legal/sub-processor or notification to the Customer via email at least thirty (30) days before engaging the Sub-processor. Customer may object to Ativion's use of a new Sub-processor by notifying Ativion promptly in writing within ten (10) days after receipt of Ativion's notice, which must be based on reasonable grounds relating to Data Protection Laws and Regulations. In the event Customer objects to a new Sub-processor, as permitted in the preceding sentence, Ativion will use reasonable efforts to cooperate with the Customer to make commercially reasonable changes to Customer's configuration or use of the Services to accommodate the Customer's objection. If Ativion cannot accommodate the Customer's objection, the parties shall come together in good faith to discuss a resolution to the objection. Such discussions shall not affect Ativion's right to use the new Sub-processor after the thirty (30) day period.

5.4. Liability. Ativion will remain liable to the Customer for ensuring Sub-processors' compliance with its data protection obligations.

6. SECURITY

6.1. Controls for the Protection of Customer Data. Ativion shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Customer Data), confidentiality and integrity of Customer Data. Ativion regularly monitors compliance with these measures. Customer acknowledges that the security measures are subject to technical progress and development and that Ativion may update or modify its technical and organizational measures from time to time, provided that Ativion will not materially decrease the overall security of the Services during a subscription term.

6.2. Data Protection Impact Assessment. Upon Customer's request, Ativion shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligation under the Data Protection Laws and Regulations to carry out a data protection impact assessment related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information and such information is available to Ativion.

7. INCIDENT MANAGEMENT AND NOTIFICATION.

7.1. Within seventy-two (72) hours of a Security Incident first becoming known to Ativion, Ativion will notify Customer by email to the most recent email address provided by Customer to Ativion. The email shall contain a summary of all facts then known about the Security Incident.

7.2 To the extent reasonably necessary, at Ativion's discretion, Ativion will provide Customer with a more-detailed notification than that required by Section 7.1, again to the most recent email address, containing at least the following information, to the extent such information is available to Ativion upon reasonable investigation:

(i) the identification and address of each Data Subject impacted by the Security Incident;

(ii) a brief description of what happened, including, without limitation, the date of the Security Incident and the date of the discovery of the Security Incident;

(iii) a description of the types of Personal Data that were involved in the Security Incident;

(iv) a detailed list of all steps that impacted Data Subjects should take to protect themselves from potential harm that will or may result from the Security Incident;

(v) a brief description of what Ativion is doing to investigate the Security Incident, mitigate the harm to Data Subjects, and protect against further Security Incidents;

(vi) a brief description of what Ativion plans to do in the immediate future to further investigate the Security Incident, mitigate the harm to Data Subjects, and protect against further Security Incident; and

(vii) complete contact information for a management-level person at Ativion for further

communications with Customer regarding the Security Incident.

7.3 Upon Customer request, Ativion will promptly notify Customer via email with updates of the items specified in Section 7.2.

7.4 Unless required by applicable Data Protection Laws and Regulations, and then only to the extent so required, Ativion will not inform any third party, including, without limitation, any impacted Data Subjects, of any Security Incident without first obtaining the prior express and unambiguous consent of Customer. Ativion acknowledges and agrees that Customer has and will have the sole right to determine: (i) whether to provide notice of any Security Incident to any of the Data Subjects, as required by law or regulation or in Customer's discretion, including, without limitation, the contents and delivery method thereof; and (ii) whether to offer any type of remedy, and the nature and extent of any such remedy, to Data Subjects.

8. RETURN AND DELETION OF CUSTOMER DATA.

Upon Customer request, Ativion shall return Customer Data in Ativion's possession to Customer and, to the extent allowed by applicable law, delete Customer Data in accordance with the ASA and applicable privacy policies (available at https://www.ativion.com/legal), unless retention of such Customer Data is required by applicable law.

9. LIMITATION OF LIABILITY

Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and Ativion, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together. For the avoidance of doubt, Ativion's and its Affiliates' total liability for all claims from Customer and all of its Authorized Affiliates arising out of or related to the Agreement and all DPAs shall apply in the aggregate for all claims under both the Agreement and all DPAs established under the Agreement, including by Customer and all Authorized Affiliates, and, in particular, shall not be understood to apply individually and severally to Customer and/or to any Authorized Affiliate that is a contractual party to any such DPA.

10. EUROPEAN SPECIFIC PROVISIONS

10.1 Standard Contractual Clauses. If Ativion or its Authorized Affiliates or Sub-processors, receives, collects, uses, stores or in any other way processes Personal Data of individuals residing in the UK or the European Economic Area as a result of the Services provided under the ASA, and Ativion receives, collects, uses, accesses, or transfers or in any other way Processes such Personal Data outside of the UK, the European Economic Area, or a country that has received an adequacy decision from the European Commission, Ativion and each applicable Authorized Affiliates and subcontractor will execute the appropriate Standard Contractual Clauses and/or international data transfer agreements (**"IDTA"**), as applicable, with all applicable parties, including Customer, if necessary.

10.2 Options for EU Standard Contractual Clauses. To the extent parties execute the Standard Contractual Clauses set forth in Schedule 2, the following term options shall apply:

- Clause 7 (Optional docking clause) is applicable;
- Clause 9 (Use of sub-processors) option 2 shall apply and the specified time or period to notice the change in sub-processor shall be set forth in Section 5 of this DPA;
- Clause 11(a) (Redress) shall not be applicable;
- Clause 17 (Governing law) option 2 shall apply, and the Parties agree that the EU Member States law shall be the law of Ireland; and
- Clause 18 (Choice of forum and jurisdiction) the Parties agree that the courts of Ireland shall have jurisdiction.

10.3 Options for UK International Data Transfer Agreements. In case of any transfers of Personal Data under this DPA under the Standard Contractual Clauses from the United Kingdom, to the extent such transfers are subject to Data Protection Laws and Regulations applicable in the United Kingdom the parties will agree to the terms set of the IDTA in Schedule 3.

11. U.S. STATE PRIVACY LAW SPECIFIC PROVISIONS

11.1 Ativion agrees that it will only Process the Personal Data for the limited and specific business purpose contemplated in the ASA, statement of work and any subsequent agreements, namely, the provision of the Services.

11.2 Ativion further agrees:

a. It shall comply with all applicable obligations under California Privacy Law and provide the same level of privacy protections as required by California Privacy Law.

b. Customer has the right to take reasonable and appropriate steps to ensure that Ativion uses the Personal Data in a manner consistent with Customer's obligations under California Privacy Law.

c. It shall notify Customer if Ativion determines that it can no longer meet its obligations under California Privacy Law.

d. Customer has the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of Customer's Personal Data.

e. Ativion will cooperate with Customer in responding to and complying with consumer requests, and Ativion will provide Customer with information necessary for Customer to comply with the requests. Alternatively, Ativion may enable Customer through its technology to comply with the requests.

11.3 Ativion agrees that it shall not:

a. Sell or share the Personal Data;

b. Retain, use, or disclose the Personal Data for any purpose other than the business purpose, namely for the provision of Services;

c. Retain, use, or disclose the Personal Data for any commercial purpose other than the business purpose;

d. Data Information outside the direct business relationship between Ativion and Customer; and

e. Combine Personal Data with personal data that Ativion receives from, or on behalf of has or receives on behalf, another person or persons, or collects from its own interaction with an individual, unless it is permitted by applicable California Privacy Law.

12. AUSTRALIAN PRIVACY SPECIFIC PROVISIONS

12.1 Scope and Applicability. This Section 12 applies where Customer is an APP Entity within the meaning of the Privacy Act 1988 (Cth) ("Australian Privacy Act") and the Personal Data processed under this DPA relates to individuals in Australia. In such circumstances, Ativion agrees to handle Personal Data in a manner that is consistent with the Australian Privacy Principles ("APPs") set out in Schedule 1 of the Australian Privacy Act, in addition to its obligations under the remainder of this DPA. Capitalised terms not otherwise defined in this Section 12 have the meanings given to them elsewhere in this DPA or in the Agreement.

12.2 Cross-Border Disclosure and APP 8 Covenant. The parties acknowledge that Customer, as the Controller, discloses Personal Data to Ativion, an overseas recipient for the purposes of section 16C and APP 8 of the Australian Privacy Act. Ativion agrees that it will not do an act, or engage in a practice, that would breach the APPs if done or engaged in by Customer. Ativion's obligations under this DPA are intended to constitute, and shall be treated as, the reasonable steps taken by Customer under APP 8.1 to ensure that the overseas recipient does not breach the APPs in relation to the Personal Data disclosed. Ativion acknowledges that, notwithstanding this covenant, Customer may remain accountable under section 16C of the Australian Privacy Act for any act or practice of Ativion that would be a breach of the APPs.

12.3 Sensitive Information. The parties acknowledge that the categories of Personal Data set out in Exhibit D may include sensitive information within the meaning of the Australian Privacy Act, including health information, information about the racial or ethnic origin of individuals, and information collected in the context of providing services to minors. Ativion agrees that it will treat such sensitive information with the additional care required by the APPs, including APP 3 (collection of sensitive information), APP 6 (use and disclosure), and APP 11 (security of personal information), and will not use or disclose sensitive information for any purpose other than the provision of the Services without Customer's prior written consent.

12.4 Purpose Limitation. Consistently with APP 6, Ativion will not use or disclose Personal Data for any purpose other than the primary purpose for which it was collected, being the provision of the Services to Customer under the Agreement, unless: (a) Customer has provided its prior written consent; (b) the secondary use or disclosure is directly related to the primary purpose and Customer would reasonably expect Ativion to use or disclose the information in that way; or (c) Ativion is required or authorised to do so by or under an Australian law or a court or tribunal order.

12.5 Security of Personal Information. Ativion confirms that the technical and organisational measures maintained under Section 6 of this DPA are intended to satisfy, and shall be

interpreted as satisfying, the obligation under APP 11 to take such steps as are reasonable in the circumstances to protect Personal Data from misuse, interference, loss, and from unauthorised access, modification, or disclosure. In applying these measures, Ativion will have regard to the OAIC's Guide to Securing Personal Information as a reference standard, in addition to any applicable UK or EU security standards referenced elsewhere in this DPA.

12.6 Notifiable Data Breaches. Where Customer is subject to the Notifiable Data Breaches scheme under Part IIIC of the Australian Privacy Act, Ativion agrees to the following obligations in addition to those set out in Section 7 of this DPA: (a) following any Security Incident notified to Customer under Section 7, Ativion will provide Customer with all information reasonably required for Customer to assess whether the Security Incident constitutes an eligible data breach under section 26WE of the Australian Privacy Act, including an assessment of the likelihood that the Security Incident will result in serious harm to any affected individual; (b) Ativion will cooperate with Customer in preparing and, if Customer determines it is required, submitting a notification to the Office of the Australian Information Commissioner ("OAIC") in the form required under Part IIIC of the Australian Privacy Act; and (c) Ativion will not notify the OAIC or any affected individual of a Security Incident without Customer's prior written consent, except where Ativion is required to do so by applicable Australian law. The parties acknowledge that Customer must notify the OAIC of an eligible data breach as soon as practicable and in any event within thirty (30) days of becoming aware of reasonable grounds to believe an eligible data breach has occurred.

12.7 Supervisory Authority. For the purposes of this DPA, where Customer is an APP Entity, the OAIC shall be treated as a competent supervisory authority in relation to the processing of Personal Data subject to the Australian Privacy Act, in addition to the supervisory authorities identified in Annex I.C of Schedule 1. Ativion agrees to cooperate with the OAIC in relation to any investigation or inquiry concerning the processing of Personal Data under this DPA, to the extent required by applicable law.

12.8 Data Subject Rights under Australian Law. Without limiting Section 3 of this DPA, Ativion will assist Customer in meeting its obligations under APP 12 (access to personal information) and APP 13 (correction of personal information). Where an individual requests access to, or correction of, their Personal Data, Ativion will provide Customer with all information and assistance reasonably required to enable Customer to respond to such a request within a reasonable time and in accordance with the Australian Privacy Act.

12.9 Destruction and De-identification. Consistently with APP 11.2, upon the expiry or termination of the Agreement, or upon Customer's earlier written request, Ativion will take such steps as are reasonable in the circumstances to destroy or permanently de-identify Personal Data that is no longer required for the provision of the Services, except where retention is required by applicable law. Any destruction or de-identification shall be carried out in accordance with Section 8 of this DPA and Ativion shall confirm to Customer in writing when it has been completed.

12.10 Amendments for Compliance with Australian Law. The parties agree to discuss in good faith any amendment to this Section 12 that may be required to address changes in the Australian Privacy Act or guidance issued by the OAIC, including any amendments arising

from the Privacy and Other Legislation Amendment Act 2024 (Cth) and any subordinate legislation or mandatory codes made under it.

13. AUDIT. Ativion will adopt and maintain policies to demonstrate compliance with this DPA and the Data Protection Laws and Regulations. No more than once every twelve (12) months, or upon reasonable request by Customer after a Security Incident or request by supervisory authority, Ativion will allow and cooperate with a reasonable audit and inspection by Customer. In the alternative, Ativion may arrange for a qualified and independent auditor to conduct an audit and inspection of Ativion's compliance which audit shall use an appropriate and accepted control standard or framework/procedure. The audit shall take place during normal business hours, subject to reasonable confidentiality obligations, and in a manner that does not unreasonably disrupt the other Party's business operation, at Customer's cost. Ativion shall provide a report of such audit to Customer upon Customer's request.

14. Amendments. Parties agree that they will discuss in good faith to negotiate amendment of this DPA to comply with model contracts, agreements, contractual terms and conditions to address changes in applicable Data Protection Laws and Regulations.

15. CONFLICTS. In the event of any conflicts between this DPA and the Agreement (except for Exhibits B and C), and any obligations in any applicable Order, the terms of this DPA shall prevail. Notwithstanding the foregoing, if there are any conflicts between the terms of Exhibits B or C, and this DPA, the terms of Exhibits B and C shall prevail. In the event of any conflict or inconsistency between the body of this DPA and the Standard Contractual Clauses in Schedule 3, the Standard Contractual Clauses/IDTA shall prevail.

List of Schedules of this DPA

Schedule 1: Standard Contractual Clauses
Schedule 2: International Data Transfer Agreement (UK ICO's Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018)

EXHIBIT E, SCHEDULE 1

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

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

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

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

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries,

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

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 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e); and

(viii) Clause 18(a) and (b).

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

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7 - Optional

Docking clause

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

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

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

MODULE TWO: Transfer controller to processor

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive

control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

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

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or

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

47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

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

(f) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[3] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(g) The data importer shall provide, at the data exporter's request, a copy of such a sub-

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

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.

(h) 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.

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

Clause 10

Data subject rights

MODULE TWO: Transfer controller to processor

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

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.

MODULE TWO: Transfer controller 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.

(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 TWO: Transfer controller to processor

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

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

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

MODULE TWO: Transfer controller to processor

(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.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

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

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE TWO: Transfer controller to processor

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the

processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[4];

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or

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

organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

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

MODULE TWO: Transfer controller to processor

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(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) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

MODULE TWO: Transfer controller to processor

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 Ireland.

Clause 18

Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

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

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

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

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

APPENDIX

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

ANNEX I

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor

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: … As set forth in ASA

Address: … As set forth in the ASA

Contact person's name, position and contact details: … As set forth in the signature line of ASA

Activities relevant to the data transferred under these Clauses: … See Exhibit D

Signature and date: … As set forth in the signature line of ASA

Role (controller/processor): controller

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

1. Name: …As set forth in ASA

Address: …As set forth in ASA

Contact person's name, position and contact details: …As set forth in the signature line of ASA

Activities relevant to the data transferred under these Clauses: See Exhibit D

Signature and date: … As set forth in the signature line of ASA

Role (controller/processor): processor

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

Categories of data subjects whose personal data is transferred

See Exhibit D.

Categories of personal data transferred

See Exhibit D.

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

Data exporter may submit special categories of data to the SCC Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which is for the sake of clarity Personal Data with information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

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

See Exhibit D.

Nature of the processing

See Exhibit D.

Purpose(s) of the data transfer and further processing

See Exhibit D.

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

See Exhibit D.

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

See Exhibit D.

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority shall be determined in accordance with Clause 13 of the SCCs.

Where applicable:

• If the Customer is established in the EEA: the supervisory authority of the Member State in which the Customer is established;
• If the Customer is established in the United Kingdom: the UK Information Commissioner's Office (ICO);
• If the Customer is established in Switzerland: the Swiss Federal Data Protection and Information Commissioner (FDPIC).

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

Data importer will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data uploaded to the SCC Services, as described in the Security, Privacy and Architecture Documentation applicable to the specific SCC Services purchased by data exporter, and accessible via email to support@ativion.com or otherwise made reasonably available by data importer. The data importer will not materially decrease the overall security of the SCC Services during a subscription term.

ANNEX III – LIST OF SUB-PROCESSORS

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

For the list of Ativion's Sub-Processors, please access: www.ativion.com/legal/sub-processor/

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: Trading name (if different): Main address (if a company registered address): Official registration number (if any) (company number or similar identifier):	Full legal name: Impero Solutions, Ltd. Trading name (if different): Ativion Main address (if a company registered address): Unit 306, 70 Wapping Wall, London E1W 3SS, UK Official registration number (if any) (company number or similar identifier):
Key Contact	Full Name (optional): Job Title:	Full Name (optional): Asta Kill Job Title: DPO

	Contact details including email:	Contact details including email: dpo@ativion.com
Signature (if required for the purposes of Section 2)		

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☑ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: Reference (if any): Other identifier (if any): Or ☐ 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: See EU SCCs
Annex 1B: Description of Transfer: See EU SCCs
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See EU SCCs
Annex III: List of Sub processors (Modules 2 and 3 only): See EU SCC

Table 4: Ending this Addendum when the Approved Addendum Changes

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

Part 2: Mandatory Clauses

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:

Mandatory Clauses	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.

EXHIBIT D
Details of the Processing

Nature and scope of processing	All processing activities required in relation to the performance of the Services under the Agreement.
Purpose of processing	Personal Data will be processed during the term of the ADA, including any data processing for transition and termination assistance. Personal Data will be deleted or returned by Ativion to Schools thereafter. Provision of the Services to you.
Duration of processing	The duration of the provision of the Services to you.
Data Subjects	Individuals whose Personal Data is included in Customer Data, include the following: Students Teachers Administrators Parents/Guardians
Categories of Personal Data	Categories of Personal Data processed will depend on the Service offerings selected: Name (First, middle, last) Email address Phone number User login/password Account information (preferences) Student ID Educational information Imprecise Geolocation Behavioral information Medical information Wellness information Service usage information Communications information Device information (IP address, hardware, software, operating system information) Monitoring of student device activity (including active windows, tabs, and usage patterns) Generation of engagement or attentiveness scores using automated analysis and providing alerts to educators (any engagement or attentiveness indicators are generated based on automated analysis of device activity and may not fully reflect a student’s actual level of engagement. Customers are responsible for interpreting such indicators in context and not relying on them as the sole basis for disciplinary or evaluative decisions)