Data Processing Addendum

This Data Processing Addendum (this "**Addendum**") is an addendum to the Terms of Service, Master Services Agreement, or other services agreement between Dura 6C LLC dba 6Connex ("**6Connex**") and the 6Connex customer signing below ("**Customer**") for the provision of the 6Connex virtual event or learning platform services (the "**Services Agreement**").

1. Definitions. As used in this Addendum, the following words have the meaning stated:

applicable law means: (i) laws applicable to the processing of personal data in the United States and each State of the United States including, without limitation, the CCPA; (ii) the GDPR, the Swiss Federal Act on Data Protection, the Data Protection Act 2018, and applicable data privacy laws of each member state of the European Union and European Economic Area, and (iii) applicable data privacy laws of other jurisdictions that the parties have expressly identified in the Services Agreement as applicable to the processing activities of 6Connex.

CCPA means the California Consumer Privacy Act of 2018;

data subject means an individual natural person who is identified or identifiable by means of the personal data, and where applicable law applies to a business, the business that is identified or identifiable by means of the personal data;

disclose means to disclose or give access to;

GDPR means the European Union General Data Protection Regulation (EU) 2016/679;

law means statutes, regulations, executive orders, and other rules issued by a government office or agency that have binding legal force;

personal data means any information about a natural person that is identified or identifiable to the natural person, either alone or in combination with other information, that 6Connex will process or have access to as part of providing the Services, including any such information that is created by means of the Services. Personal data includes "personal data" as that term is defined in the GDPR and "personal information" as that term is defined in the CCPA;

personnel means the employees and individual contractors under the direct supervision of the person referred to;

process when used with respect to data means: (i) to record, store, organize, structure, analyze, query, modify, combine, encrypt, display, disclose, transmit, receive, render unusable, or destroy, by automated means or otherwise, and (ii) to provide cloud or other remote technology hosting services for applications or services that do any of the foregoing, and (iii) any other use or activity that is defined or understood to be processing under applicable law. The terms process, processing and their variants should be construed broadly in light of the parties' goal to protect personal data;

security event means any of the following: (i) unauthorized processing or other use or disclosure of personal data, (ii) unauthorized access to or acquisition of personal data or the systems on which personal data is processed; (iii) any significant corruption or loss of personal data that 6Connex is unable to repair within a minimal period of time, and (iv) any event that has or is reasonably likely to significantly disrupt the processing of the personal data as contemplated by the Services Agreement;

sub-processor and sub-processor agreement have the meaning given in Section 4 (*Disclosure to Third Parties*) below;

2. **General**. As between 6Connex and Customer: (i) Customer controls the purpose and means of processing of personal data, and is the "controller" under the GDPR and the "business" under the CCPA, and (ii) 6Connex is authorized to process the personal data only as instructed by Customer, including as described in the Services Agreement and this Addendum, and is the "processor" under the GDPR and the "service provider" under the CCPA. 6Connex shall comply with the requirements stated in this Addendum, and any additional or more stringent requirements or restrictions applicable to processors and service providers under applicable law.

3. **Permitted Use and Disclosure**. 6Connex shall not process personal data except as follows:

   (i) as necessary to provide the Services in accordance with the Services Agreement, subject to Section 4 (*Disclosure to Third Parties*); or

   (ii) in accordance with Customer's written instructions;

   (iii) as required by applicable law, subject to Subsection 4.2 (*Legally Required Disclosure*); or

   (iv) as necessary to comply with legal requirements for records retention or for internal administrative purposes related to the provision of the Services, except to the extent such processing would violate restrictions under applicable law.

For clarity, 6Connex may not sell the personal data as that term is used in the CCPA.

4. **Disclosure to Third Parties.**

   4.1 Disclosure to Sub-processors. Customer hereby consents to 6Connex's use of the sub-processors identified on Schedule 1. 6Connex may disclose Customer's personal data to additional sub-processors provided that: (i) it provides advance written notice of the sub-processor and the sub-processing; and (ii) 6Connex has conducted and documented appropriate due diligence to confirm that the sub-processor has sufficient operational and financial strength to provide the level of protection for personal data that is required by the Services Agreement and this Addendum. In all events, each sub-processor shall be subject to written obligations at least as stringent as those stated in this Addendum to protect the personal data and to provide assistance as necessary for 6Connex to meet its obligations to Customer such as appropriate notice and audit terms, and cooperation with respect to data subject requests. Each sub-processor agreement must include a requirement that the sub-processor require its sub-processors at any tier to meet requirements applicable to 6Connex and sub-processors under this this Addendum. 6Connex shall be responsible for the acts and omissions of each sub-processor (direct and indirect at any tier) in violation of this Addendum to the same extent as for 6Connex's own acts and omissions. If Customer reasonably objects to a sub-processor added after the effective date of this Addendum, 6Connex shall not use the sub-processor to process Customer's personal data, or if that is not commercially feasible, shall permit Customer to terminate the Services Agreement without liability.

   4.2 Legally Required Disclosures. 6Connex may disclose personal data as required by a subpoena or other compulsory legal process provided that: (i) it gives Customer as much advance notice of the disclosure as is reasonably practical under the circumstances (unless notice is prohibited by law), (ii) it discloses only the personal data that it is legally compelled to disclose, and (iii) it cooperates, at Customer's expense, with Customer's reasonable requests to avoid or limit disclosure, or if 6Connex is not permitted to give notice of the disclosure, it uses reasonable efforts to challenge or narrow the requirement in accordance with applicable law.

4.3 Requests from Data Subjects. 6Connex shall promptly notify Customer if 6Connex receives a request from a data subject to disclose, provide a copy, modify, block, or take any other action with respect to the personal data, unless notice is prohibited by applicable law. 6Connex shall not independently take any action in response to a request from a data subject without Customer's prior written instruction unless required by law. 6Connex shall cooperate with Customer's reasonable requests for access to personal data and other information and assistance as necessary to respond to a request or complaint by a data subject.

5. Protection of Personal Data. 6Connex shall protect personal data from unauthorized acquisition, use, disclosure, loss, corruption, and unavailability using appropriate physical, technical, organizational, and administrative safeguards, and will require each of its sub-processors to do the same. 6Connex is ISO27001 certified and meets the requirements of this Section by adhering to ISO27001 standards.

6. Cross-Border Transfer of Personal Data. The parties contemplate that Customer will transfer the personal data covered by this DPA to 6Connex's services environment located in the United States. Transfer to and from the U.S. is made via global networks managed by 6Connex's content management sub-processors and may entail temporary storage outside of the U.S. The following additional terms apply to personal data covered by the GDPR: (i) Customer is the "exporter" and 6Connex is the "importer" of the personal data transferred to the United States, (ii) the standard contractual clauses for the transfer of personal data to processors established in third countries under the Directive or the GDPR or its national equivalents "**Standard Contractual Clauses**") are attached to this DPA as Schedule 2 and are incorporated in this DPA by this reference, and (iii) if there is a conflict between the Standard Contractual Clauses and the body of this DPA, the Standard Contractual Clauses shall control; and (iv) Customer represents and warrants to 6Connex that the transfer of the data is permitted under Article 49 of the GDPR.

7. Notice of Security Event. 6Connex shall provide notice as provided in Section 12.2 (*Notices*) without undue delay and all events within seventy-two (72) hours of discovering that a security event has occurred. 6Connex's notice shall include the following information to the extent it is reasonably available to 6Connex at the time of the notice, and 6Connex shall update its notice as additional information becomes reasonably available: (i) the dates and times of the security event; (ii) the facts that underlie the discovery of the security event, or the decision to begin an investigation into a suspected security event, as applicable; (iii) a description of the personal data involved in the security event, either specifically, or by reference to the data set(s), including the approximate number of data subjects concerned and the categories and approximate number of personal data records concerned; (iv) the measures planned or underway to remedy or mitigate he vulnerability giving rise to the security event; (v) the name and contact details of 6Connex's data protection officer or other contact point where more information can be obtained; (vi) the likely consequences of the personal data breach. 6Connex shall promptly provide other information regarding the security event or suspected security event that Customer may reasonably request.

8. Mitigation/Investigation/Remediation. 6Connex shall take those measures available, including measures reasonable requested by Customer, to address a vulnerability giving rise to a successful security event, both to mitigate the harm resulting from the security event and to prevent similar occurrences in the future. 6Connex shall cooperate with Customer's reasonable requests in connection with the investigation and analysis of the security event, including a request to use a third- party investigation and forensics service. 6Connex shall retain all information that could constitute evidence in a legal action arising from the security event and shall provide the information to Customer on Customer's request. Except to the extent required by law in the written and reasonable opinion of 6Connex's counsel, 6Connex shall not disclose to any person the existence of a security event or suspected security event or any related investigation without Customer's prior written consent.

9. Cooperation. 6Connex shall cooperate with Customer's reasonable requests information and assistance in connection with (i) Customer's internal security and privacy risk assessments, and (ii) any audits or verifications of Customer's privacy and security policies and practices by Customer's customers, regulators, or other stakeholders.

10. Records and Audit. 6Connex shall keep reasonable records of the personal data processing activities as necessary to verify its compliance with this Addendum and shall preserve the records for at least two (2) years from the date of the events reflected in the records. 6Connex shall provide Customer or its or its customers' regulatory authorities, or any of their independent third-party auditors, with access to its relevant records, systems, facilities and personnel for the purpose of auditing or verifying compliance with this Addendum promptly on request, provided that any such audit or verification shall be performed on reasonable advance notice and shall not unduly disrupt 6Connex's operations. If any audit or verification reveals a failure to comply with any requirement set forth in this Addendum, 6Connex shall promptly provide a plan to remediate the failure and begin remediation. 6Connex shall bear all reasonable costs for controlled reverification of the remediation of any such issue.

11. Return or Destruction of personal data. On expiration of the Services Agreement or any earlier termination, or on Customer's request at any time, 6Connex shall return or destroy any personal data that is within its control; provided, however, that:

(i) It shall retain personal data that it is required to retain by the express terms of the Service Agreement or by applicable law;

(ii) on Customer's request, 6Connex shall not destroy the personal data until it has given Customer access to the personal data for a reasonable period of time as necessary to complete an orderly migration of the personal data to Customer's or a substitute provider's systems;

(iii) if Customer requires 6Connex to return or destroy personal data prior to the expiration or termination of the Services Agreement, 6Connex is excused from performing those Services that it is unable to perform as a result of the return or destruction; and

(iv) 6Connex is not required to return or destroy personal data to the extent it is expressly permitted to retain the personal data under Section 3 (*Permitted Use and Disclosure*) above, or if destruction or return is commercially or technically infeasible. 6Connex shall provide a written description of any personal data that it proposes to retain with a statement of the reasons for retention, and shall cooperate with Customer's reasonable requests to address record keeping needs or to overcome infeasibility issues. On Customer's request, 6Connex shall provide a certification (signed by its executive offer) that return or destruction has been completed in accordance with this Addendum.

12. General.

12.1 Term and Termination. This Addendum is effective as of the Effective Date and shall continue in effect for so long as 6Connex continues to have access to or process personal data. This Addendum survives the expiration or termination of the Services Agreement for so long as 6Connex has access to or processes personal data. If 6Connex violates this Addendum, Customer may terminate this Agreement and the Services Agreement for breach. Customer may, in its sole discretion, give 6Connex an opportunity to cure any violation, and may suspend 6Connex's access to or processing of the personal data during the cure period.

12.2 Notices. Except as otherwise expressly stated otherwise in this Addendum, notices required under this Addendum shall be given in writing in the manner required in the Services Agreement. If Customer has provided a privacy notice contact, 6Connex shall also notify Customer's privacy notice contact.

12.3 Precedence and Interpretation. This Addendum is intended to supplement the Services Agreement. If there is a conflict between this Addendum and the Services Agreement, this Addendum controls. If there is a conflict between the terms of Schedule 1 to this Addendum and the body of this Addendum, Schedule 1 controls. Any ambiguity in this Addendum as to a matter covered by applicable law should be interpreted in a way that conforms to applicable law. For clarity, this Addendum is subject to the liability caps and damages exclusions stated in the Services Agreement.

12.4 Rights in Data. As between Customer and 6Connex, Customer retains all right, title and interest in and to the personal data.

12.5 Assignment, Change in Control. 6Connex must give Customer advance written notice of any transaction that will result in a change of control of 6Connex or any sub-processor, or assignment or transfer of this Agreement or any sub-processor agreement. If Customer reasonably concludes that the following the transaction the 6Connex or its successor does not have the operational or financial strength to perform the 6Connex's obligations under this Agreement, Customer may terminate the Services Agreement without liability. The requirements of this Subsection are in addition to any requirements stated in the Services Agreement and apply notwithstanding anything to the contrary in the Services Agreement.

12.6 Confidential Information. Any additional or more stringent protections or remedies available with respect to information defined as "confidential information" or with like term under the Services Agreement apply to personal data.

SIGNATURES ON FOLLOWING PAGE

Dura 6C, LLC dba 6Connex

Name:

Title:

Date Signed:

[Customer’s full legal name]

Name:

Title:

Date Signed:

Attach: Schedule 1, Processing Details

Data Processing Addendum, Schedule 1
Processing Details

Purpose of Processing: the provision of virtual event or learning platform services

Categories of data subjects:

(i) Customer’s staff who interact with 6Connex to purchase and use the Services; and

(ii) users of the Customer’s instance of the 6Connex virtual event or learning platform services, such as the attendees at Customer’s virtual events or users of online course materials

Categories of personal data:

(i) as to Customer’s staff, name and business contact information, such as email address and phone number, and user names and passwords for authenticating on the administrative features of the Services; and

(ii) as to users of the Customer’s instance of the 6Connex virtual event or learning platform services: (i) IP address; (ii) user name and other authentication credentials established as part of registration for event or learning platform; (iii) contact information such as email, phone number, and physical address; (iv) navigation path and duration of visit on the 6Connex platform generally and on parts of the platform, such as virtual event features used or visited and learning materials accessed.

Categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organizations: 6Connex service providers:

- Amazon Web Services, Inc., Seattle, Washington, infrastructure hosting and related services
- Akamai Technologies, Inc., Cambridge Massachusetts, content delivery network services

Third countries or international organizations to which the personal data will be transferred, if applicable:

Personal data may be transferred through countries other than the origin country and the United States by Akamai Technologies, Inc. as part of providing global content delivery network services

Data Processing Addendum, Schedule 2

STANDARD CONTRACTUAL CLAUSES
Controller to Processor Modules
((EU)2021/914 of 4 June 2021

SECTION I

Clause 1 Purpose and scope

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

(b) The Parties:

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

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

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

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.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, 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 – Clause 8.1(b), 8.9(a), (c), (d) and (e);
(iii) Clause 9 – Clause 9(a), (c), (d) and (e);
(iv) Clause 12 –Clause 12(a), (d) and (f);
(v) Clause 13;
(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);
(viii) Clause 18 – 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 Docking clause

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8 Data protection safeguards

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

8.1 Instructions

(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 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 (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

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

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

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

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

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

8.9 Documentation and compliance

(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

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.
(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10 Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.
(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11 Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.
(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

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

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12 Liability

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

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

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

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

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

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

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

Clause 13 Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

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

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

Clause 14 Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

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

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

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

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

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

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

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

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

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

15.1 Notification

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

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

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

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

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

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

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 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

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).

Clause 18 Choice of forum and jurisdiction

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

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

ANNEX I

A. LIST OF PARTIES

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

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

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

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

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.

ANNEX III

LIST OF SUB-PROCESSORS

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

1.Name: … Amazon Web Services, Inc.

Address: 400 9th Ave. N., Seattle, Washington, USA

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

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): …Platform hosting services

2. Name: … Akamai Technologies, Inc..

Address: …145 Broadway, Cambridge, Massachusetts, USA

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

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