Data Processing Addendum

This Data Processing Addendum (this "**Addendum**") is an addendum to the 6Connex Terms and Conditions at https://www.6connex.com/legal/, as it may be updated from time to time, or other agreement between the 6Connex entity identified in the signature block below ("**6Connex**") and the 6Connex customer (the "**Customer**") for 6Connex's Platform Services (the "**Services Agreement**").

This Addendum is comprised of the following parts:

Cover this page

Part 1 Parties

Part 2 Description of Transfer, Processing Details

Part 3 Description of 6Connex's Technical and Organizational Security Measures;

Part 4 List of 6Connex Subprocessors

Part 5 Generally Applicable Terms

Appendix 1 to Part 5 – EU Standard Contractual Clauses, Controller to Processor; and,

Appendix 2 to Part 5 – UK Standard Contractual Clauses, Processors

Capitalized terms used in this Data Processing Addendum have the meaning given in Section 1 (*Definitions*) of Part 5, Generally Applicable Terms, unless otherwise stated.

The parties signing the Services Agreement intend for their signatures on the Agreement to evidence acceptance of all parts of this Addendum, as applicable, and to serve as the required signatures as data importer (for 6Connex) and data exporter (for Customer) on each of the EU Standard Contractual Clauses (the "EU SCC") and UK Standard Contractual Clauses (the "UK SCC"), including those appendices of each of them that are required to be signed.

Part 1, Parties
The information in this Part 1 is intended to serve as Part A of Annex 1 of the EU SCCs, and the required information on Page 1 of the UK SCCs.

Parties:

Name of Data Importing Organization: Dura 6C, LLC dba 6Connex	***Name of Data Exporting Organization***: [insert full name of customer]
Address: 425 Soledad Street San Antonio, TX 78205	***Address***: [customer to insert]
Telephone: +1.210.890-5769	***Telephone***: [customer to insert]
Fax: none	***Fax***: none
Email: privacy@6connex.com	***Email***: [customer to insert]
	Customer is established in [insert name of member state of the EU or EEA, or UK or Switzerland]
Contact person's name, position and contact details: the individual signing this Addendum on Page 1 as their name is shown in the signature block on Page 1, the "title" as shown on Page 1 of this Addendum, and the contact details shown above in this Part 1.	***Contact person's name, position and contact details***: the individual signing this Addendum on Page 1 as their name is shown in the signature block on Page 1, the "title" as shown on Page 1 of this Addendum, and the contact details shown above in this Part 1.
Activities relevant to the data transferred under these Clauses: processing of personal data as part of providing services under the Services Agreement and the administration of the exporter's account, as more specifically described in Part 2 of this Addendum	***Activities relevant to the data transferred under these Clauses:*** transfer of personal data to importer for its use in providing services under the Services Agreement and the administration of the exporter's services account, as more specifically described in Part 2 of this Addendum
Other information necessary in order for the contract to be binding (if any): none	**Other information necessary in order for the contract to be binding (if any)**: [none, unless customer states otherwise here]
Role: Processor or Subprocessor	***Role***: Controller or processor or subprocessor

The Date of the EU SCCs and the UK SCCs is the Effective Date of this Addendum as stated on Page 1 of this Addendum.

Part 2, Description of Transfer, Details of Processing

Data exporter
The data exporter is (please specify briefly activities relevant to the transfer):

[Customer to complete]

Data importer
The data importer is (please specify briefly activities relevant to the transfer):

Provider of online platform services and mobile applications for organizing and holding interactive virtual events.

The services may include features that enable end users to discover interactive virtual events offered on the online platform by event organizers and interacting with other end users in connection with the events offered.

Categories of data subjects (whose personal data is transferred):

(i) Customer personnel whose personal data is provided to importer for the purposes of establishing and maintaining the Customer's account; and

(ii) End users who interact with the online event platform or mobile application, such as to purchase event tickets, attend events, use or contribute content, and communicate with event organizers or other platform end users.

Categories of personal data transferred:

(i) As to customer personnel, name, business contact information, business IP address, service account names and passwords who are assigned by Customer to manage the Customer's accounts with importer; and

(ii) As to end users who interact with the online event platform or mobile application: (A) IP address; (B) user name and other authentication credentials established as part of ticket purchase or platform registration; (C) contact information such as email, phone number, and physical address; (D) navigation path and duration of visit on the online platform generally and on specific parts of the platform, such as event features used or visited and content; (E) payments made for services available through the platform, (F) interaction with other users, (G) personal data that may be included in recommendations, comments, and messages published on the platform or exchanged in communications with other end users.

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 transfer or additional security measures.

The Services are not intended for use in processing sensitive data types; Customer is not permitted to knowingly transfer any sensitive data to 6Connex.

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

Data is transferred on a continuous basis throughout the term of the Services Agreement

Nature of Processing:

Processing as necessary to provide 6Connex' services in accordance with the service agreement between Customer and 6Connex and related administrative purposes, and as otherwise permitted by the Service Agreement

Purpose of the data transfer and further processing:

To enable 6Connex to provide the services and administer the Customer's account in accordance with the Service Agreement.

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

For the term of the Services Agreement and for a reasonable period following expiration or termination of the Services Agreement as necessary to facilitate an orderly transfer of personal data to the exporter; and as to personal data transferred for the purpose of administering Customer's account (such as business contact information) for a reasonable period following expiration or earlier termination of the Services Agreement as consistent with 6Connex' reasonable and industry standard record keeping practices, to the extent such practices do not violate applicable law.

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

Subject Matter and nature of processing: see Part 4, List of Subprocessors
Duration of processing: as described above for 6Connex

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

Sub-processors described in Part 4 of the Addendum; personnel of 6Connex's affiliates in the European Economic Area and United Kingdom

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

Transfer to and from the U.S. is made via global networks managed by 6Connex' content management sub-processors and may entail temporary storage outside of the U.S.

Technical and Organizational Security Measures

See Part 3 of the Addendum.

Part 3, Description of 6Connex's Technical and Organizational Security

The technical and organizational measures are implemented by 6Connex in accordance with Art 32 GDPR. 6Connex strives to continuously improve on these measures. 6Connex maintains an active ISO 27001 certification.

1. Confidentiality

1.1. Physical Access Control

Measures suitable for preventing unauthorized persons from gaining access to data processing systems with which personal data are processed or used.

6Connex's workforce is fully remote with Amazon Web Services (AWS) providing the physical security aspects of access to it's Datacenter(s).

Technical Measures

- AWS

Organizational Measures

- AWS
- Physical Security Policy

1.2. Logical Access Control

Measures to protect against data processing systems from being used by unauthorized persons.

Technical Measures

- Login with username + strong password
- Anti-Virus Software Servers
- Anti-Virus Software Clients
- Two-factor authentication
- Firewall (WAF) - AWS
- Intrusion Detection Systems
- Use of VPN for remote access
- Encryption of data carriers
- Automatic desktop lock
- Encryption of Endpoints
- Encryption of Databases + Backups

Organizational Measures

- User permission management
- Creating user profiles
- Central password assignment
- Access Control Security Policy
- Work instruction IT user regulations
- Work instruction operational security
- Security Awareness Training
- Mobile Device Policy

1.3. Authorization Control

Measures designed to ensure that those authorized to use a data processing system can only access the data subject to their access authorization and that personal data cannot be read, copied, modified or removed without authorization during processing, use and after storage.

Technical Measures

- Physical deletion of data carriers
- Logging of accesses to applications, specifically when entering, changing, and deleting data
- SSH encrypted access

Organizational Measures

- Use of authorization concepts
- Minimum number of administrators
- Management of user rights by administrators
- Access Control Security Policy

- Certified SSL encryption
- Security Awareness Training
- Information Handling Training / Policy

1.4. Separation Control

Measures designed to ensure that data collected for different purposes can be processed separately, such as by logical and physical separation of the data.

Technical Measures

- Separation of productive and test environment
- Multi-tenancy of relevant applications
- VPC segmentation (AWS)
- Network Segmentation
- Staging of development, test and production environment
- Separation of productive and test Data

Organizational Measures

- Control via authorization concept
- Determination of database rights
- Information Security Policy
- Data Protection Policy
- Work instruction operational security
- Work instruction security in software development
- Secure Development Lifecycle Development (SDLC)

1.5. Pseudonymization

The processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organizational measures.

Technical Measures

- In case of pseudonymization: separation of the allocation data and storage in separate systems (encrypted)
- Separation of productive and test Data

Organizational Measures

- Defined Data Anonymization /Deletion Process
- Information Security Policy
- Information Classification Policy

2. Integrity

2.1. Transfer Control

Measures designed to ensure that personal data cannot be read, copied, altered or removed by unauthorized persons during electronic transmission or while being transported or stored on data media, and to enable 6Connex to verify and establish to entities to which personal data are intended to be transmitted by data transmission equipment.

Technical Measures

- Use of VPN
- Logging of accesses and retrievals
- Use of encrypted connections such as HTTPS/SSL and secure cloudstores
- Prevention of the usage of USB/External

Organizational Measures

- Survey of regular retrieval and transmission processes
- Acceptable Use Policy
- Information Security Policy (ISO27001 Compliant ISMS)

Storage Devices on Endpoints
- SAML
- Hash/Salted Password Storage
- Data Protection Policy

2.2. Input Control

Measures designed to ensure that PII modified or removed from data processing systems is specifically limited. Input control is achieved through logging, which can take place at various levels (e.g., operating system, network, firewall, database, application).

Technical Measures
- Technical logging of the entry, modification and deletion of data
- Manual or automated control of the logs (according to strict internal specifications)

Organizational Measures
- Survey of which programs can be used to enter, change or delete which data
- Traceability of data entry, modification and deletion through individual user names (not user groups)
- Assignment of rights to enter, change and delete data based on authorization/Role-based requirements only
- Clear responsibilities for deletions + Process
- Information Security Policy (ISO27001 Compliant ISMS)

3. Availability and Resilience

3.1. Availability Control

Measures designed to ensure that personal data is protected against accidental destruction or loss (UPS, air conditioning, fire protection, data backups, secure storage of data media, virus protection, raid systems, disk mirroring, etc.).

Technical Measures
- Fire and smoke detection systems
- Fire extinguisher server room
- Server room monitoring temperature and humidity
- Server room air-conditioning
- UPS system and emergency diesel generators
- Protective socket strips server room
- RAID system / hard disk mirroring
- Video surveillance server room
- Alarm message in case of unauthorized access to server room

Organizational Measures
- Regular Backups
- Disaster Recovery plan (AWS)
- Disaster Recovery plan (6Connex)
- Information Security Policy (ISO27001 Compliant ISMS)
- Incident Response Policy

- Availability Zones (AWS) for Failover

3.2. Recoverability Control

Measures designed to rapidly restoring the availability of and access to personal data in the event of a physical or technical incident.

Technical Measures

- Backup monitoring and reporting
- Availability Zones (AWS) for Failover

Organizational Measures

- Recovery concept
- Control of the backup process
- Regular testing of data recovery and logging of results
- Disaster Recovery plan (AWS)
- Disaster Recovery plan (6Connex)
- Information Security Policy (ISO27001 Compliant ISMS)
- Incident Response Policy

4. Procedures for regular Review, Assessment and Evaluation

4.1. Data Protection Management

Technical Measures

- Central documentation of all data protection regulations with access for employees
- Security certification (ISO 27001)
- A review of the effectiveness of the technical and organization security measures ("TOMS") is carried out at least annually and TOMs are updated
- Annual Risk Assessment(s)

Organizational Measures

- Data Protection Officer, DPO
- Annual Security Awareness Training
- Regular awareness trainings at least annually
- Data Protection Impact Assessment (DPIA) is carried out as required
- Processes regarding information obligations according to Art 13 and 14 GDPR established
- Formalized process for requests for information from data subjects is in place
- Data protection aspects established as part of corporate risk management
- ISO 27001 certification of key parts of the company including data center operations and annual monitoring audits

4.2. Incident Response Management

Support for security breach response and data breach process.

Technical Measures

Organizational Measures

- Use of firewall (AWS WAF)
- Use of spam filter
- Use of AntiVirus/AntiMalware and alerting
- Intrusion Detection System (IDS)

- Documented process for detecting and reporting security incidents / data breaches
- Formalized procedure for handling security incidents
- Involvement of DPO and Security Team in security incidents and data breaches
- Documentation of security incidents and data breaches
- A formal process for following up on security incidents and data breaches
- Information Security Policy (ISMS)
- Data Protection Policy
- Annual Security Awareness Training

4.3. Data Protection by Design and by Default

Measures pursuant to Art 25 GDPR that comply with the principles of data protection by design and by default.

Technical Measures

- Limitation of the amount of PII Collected
- Encryption (Data in Transit HTTPS/SSL)
- Encryption (Data at rest AES-256)

Organizational Measures

- Data Protection Policy (includes principles "privacy by design / by default")
- Annual OWASP Secure Development Security assessment via third-party

4.4. Order Control (outsourcing, subcontractors and order processing)

Measures to ensure that personal data processed on behalf of the client can only be processed in accordance with the client's instructions.

Technical Measures

- Monitoring of remote access by external parties
- VPN + Two-Factor Authentication
- Monitoring of subcontractors according to the principles and with the technologies according to the preceding sections

Organizational Measures

- Work instruction supplier management and supplier evaluation
- Prior review of the security measures taken by the contractor and their documentation
- Selection of the contractor under due diligence aspects (especially with regard to data protection and data security)
- Conclusion of the necessary data processing agreement on terms meeting regulatory requirements for sub processors
- Framework agreement on contractual

data processing within the group of companies
- Written instructions to the contractor
- Agreement on effective control rights over the contractor and intellectual property rights

5. Certifications

6Connex maintains its compliance with ISO27001.

Measures overview:

Measure	Standard
Physical Access Control	ISO 27001 certified
Logical Access Control	ISO 27001 certified
Authorization Control	ISO 27001 certified
Separation Control	ISO 27001 certified
Pseudonymization	ISO 27001 certified
Transfer Control	ISO 27001 certified
Input Control	ISO 27001 certified
Availability Control	ISO 27001 certified
Recoverability Control	ISO 27001 certified
Data Protection Management	ISO 27001 certified
Incident Response Management	ISO 27001 certified
Privacy by Design and by Default	ISO 27001 certified
Order Control	ISO 27001 certified
Organization	ISO 27001 certified

Part 4 – List of 6Connex Sub-processors

- Amazon Web Services, Inc., Seattle, Washington, infrastructure hosting and related services
- Akamai Technologies, Inc., Cambridge Massachusetts, content delivery network services
- Webinar.net, Pleasanton, California, web-casting services
- TalkPoint Holdings, LLC (PGi), Alpharetta, Georgia, web-casting services

Part 5 of Data Processing Addendum, Generally Applicable Terms

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 UK GDPR, the Swiss Federal Act on Data Protection and applicable data privacy laws of each member state of the European Union and European Economic Area ("**applicable European law**"), 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;

EU SCCs means the standard contractual clauses for the transfer of personal data from controllers to processors or from processors to processors, as applicable, established in third countries under GDPR or its national equivalents adopted by the EU Commission in its Implementing Decision (EU) 2021/914;

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; and

UK GDPR means the GDPR as adopted by the United Kingdom and supplemented by the Data Protection Act of 2018; and

UK SCCs means the standard contractual clauses for international transfers from controllers to processors adopted by the UK Information Commissioner's Office.

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' use of the sub-processors identified on Part 4 of this Addendum. 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 the physical, technical, organizational, and administrative safeguards described on Part 3 of this Addendum or measures more stringent, and will require each of its sub-processors to do the same.

6. Cross-Border Transfer of Personal Data. The parties contemplate that Customer will transfer personal data covered by applicable European law 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-processor 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 EU SCC's and the UK SCC's are attached to this Part 5 as Annex 1 and Annex 2 (collectively the "SCC's") and are incorporated in this DPA by this reference, (iii) if there is a conflict between the SCC's and the body of this DPA, the SCC's 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 Appendix 1 – EU SCCs to this Addendum and the body of this Addendum, Appendix 1 – EU SCCs 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.

Data Processing Addendum, Part 5, Appendix 1 – EU SCCs

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); .

(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 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.

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 importe8.7 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 the jurisdiction identified in Part 1.

Clause 18 Choice of forum and jurisdiction

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

(b) The Parties agree that those shall be the courts of the jurisdiction identified in Part 1.
(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

See Part 1 of the Addendum

B. DESCRIPTION OF TRANSFER

See Part 3 of the Addendum

C. COMPETENT SUPERVISORY AUTHORITY

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

The supervisory authority in the jurisdiction identified in Part 1.

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

See Part 3 of the Addendum

ANNEX III - LIST OF SUB-PROCESSORS

See Part 4 of the Addendum

Standard Contractual Clauses – UK, Controllers to Processors

Clause 1 Definitions

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'Commissioner' shall have the same meaning as in the UK GDPR;

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system covered by UK adequacy regulations issued under Section 17A Data Protection Act 2018 or Paragraphs 4 and 5 of Schedule 21 of the Data Protection Act 2018;

(d) 'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the UK;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2 Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3 Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4 Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the Commissioner and does not violate the applicable data protection law;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the Commissioner if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5 Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the Commissioner with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the Commissioner;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;
(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6 Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.
3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7 Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the Commionser;
   (b) to refer the dispute to the UK Courts.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8 Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the Commissioner if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the Commissioner has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9 Governing Law

The Clauses shall be governed by the law of the Country of the United Kingdom in which data exporter is established, namely England and Wales.

Clause 10 Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from (i) making changes permitted by Paragraph 7(3) and 4 of Schedule 21 Data Protection Act 2018; or (ii) adding clauses on business related issues where required (as long as they do not contradict the Clause).

Clause 11 Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement

with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Country of the UK where the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the Commissioner.

Clause 12 Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the Commissioner, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

See Part 2 of the Addendum

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

See Part 3 of the Addendum