Data Protection Addendum

This Data Protection Addendum ("DPA") is incorporated by reference into the master services agreement and all related orders for Services between Mediaocean LLC and its Affiliates ("Supplier") and [Customer name] (the "Customer") named therein. This DPA is entered into as of the later of the dates beneath the parties' signatures below.

This DPA is supplemental to the Agreement and sets out the terms that apply when Personal Data (defined below) is processed by Supplier under the Agreement. The purpose of the DPA is to ensure such processing is conducted in accordance with Data Protection Laws, and with due respect for the rights and freedoms of individuals whose Personal Data are processed.

DATA PROCESSING TERMS

In providing the Services to the Customer pursuant to the Agreement, Supplier may process Personal Data on behalf of the Customer. Supplier will comply with the provisions in this DPA with respect to its processing of any Personal Data.

1 Definitions

1.1 For the purpose of this DPA:

a) Affiliates has the same meaning ascribed to it in the Agreement and, if not defined in the Agreement, the term means any legal entity directly or indirectly controlling, controlled by or under common control with a party, where control means the ownership of a majority share of the stock, equity or voting interests of such entity.
b) Agreement means the contractual agreement(s) including services agreements and all related orders between Supplier and Customer.
c) Client has the same meaning as ascribed to it in the Agreement.
d) Controller means the entity which, alone or jointly with others, determines the purposes and means of processing of Personal Data.
e) Customer means the party to both the Agreement and this DPA that has access to the Services.
f) Customer Data means any data, information or material originated by the Customer that the Customer submits to Supplier, collects through its use of the Services or provides Supplier in the course of using the Services.
g) Data Protection Laws means all laws and regulations, including laws and regulations of the European Union, the European Economic Area, their member states and the United Kingdom, applicable to the processing of Personal Data under the Agreement, including (where applicable) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR), the UK GDPR and the Data Protection Act 2018, and the California Consumer Privacy Act (CCPA).
h) Data Subject means the individual to whom Personal Data relates.
i) EEA means European Economic Area, which constitutes the member states of the European Union and Norway, Iceland and Liechtenstein.
j) Supplier means the Mediaocean entities that are a party to both the Agreement and this DPA.
k) Personal Data means any Customer Data relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic cultural or social identity of that natural person.

l) Processor means an entity which processes Personal Data on behalf of the Customer.
m) Services means the services provided by Supplier to the Customer under the Agreement.
n) Standard Contractual Clauses (SCCs) means the Standard Contractual Clauses for the transfer of personal data to processors established in third countries that have not received an applicable adequacy decision in the form set out by European Commission Decision 2021/914/EU and approved for use in data transfers under the UK GDPR which can be found at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en#ntc12-L_2021199EN.01003701-E0012 (the "SCCs").
o) Sub-processor means an Affiliate or third party processor engaged by Supplier to process Personal Data on Supplier's behalf.
p) UK means the United Kingdom.
q) UK Addendum means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses in force 21 March 2022 in Exhibit 1. The UK Addendum shall supplement the SCCs for transfers outside of the UK. The UK Addendum located in is hereby incorporated by reference. The UK Addendum is hereby incorporated by reference.

2 Applicability of DPA

2.1 This DPA shall apply only to the extent that Supplier processes Customer Data which includes Personal Data.

3 Data Processing

3.1 Controller/Processor Designation. The parties hereby acknowledge and agree that Customer is the Controller with respect to the Personal Data provided to direct to Supplier by an individual user of the Platform.

The Parties acknowledge and agree that Supplier is [check as applicable]:

- a Processor of such Personal Data.
- an Independent Controller of such Personal Data.
- A Service Provider as defined under the California Consumer Privacy Act (CCPA).

3.2 For Processors, Additional Service Provider Designation. Supplier hereby acknowledges that in addition to its role as a Processor, it will also act as a "Service Provider" of Customer's Personal Data under the California Consumer Privacy Act (CCPA). Supplier hereby certifies that it does not receive Customer's Personal Information (as defined by the CCPA) as consideration for any services and does not otherwise derive value from the processing or use of Customer's Personal Information other than the value derived as a result of Supplier's direct business relationship with Customer. Supplier certifies that it does not and will not sell Customer's Personal Information, as the term "sell" is defined under the CCPA, and acknowledges that it may not retain, use, or disclose Customer's Personal Information except as is necessary to provide services to Customer. Supplier certifies that it understands the rules, requirements and definitions of the CCPA and shall refrain from taking any action that may qualify as selling Customer Personal Information under the CCPA.

3.3 Purpose Limitation. Supplier shall process Personal Data for the purposes set forth in the Agreement and only in accordance with the lawful, documented instructions of Customer, except where otherwise required by applicable law. The parties agree that this DPA and the Agreement constitute Customer's documented instructions to Supplier for the processing of Personal Data ("Documented Instructions"). The Subject-Matter, Nature, Purpose and Duration of Data Processing along with Categories of Data Subjects and Types of Personal Data are documented

in Annex 1B attached. Any processing required outside the scope of these Documented Instructions will require prior written agreement of the parties.

3.4 Compliance. Customer, as Controller, shall be responsible for ensuring that, in connection with Customer Data and the Services:

a it has complied, and will continue to comply, with all applicable laws relating to privacy and data protection, including the Data Protection Laws; and

b it has, and will continue to have, the right to transfer, or provide access to, the Personal Data to Supplier for processing in accordance with the terms of the Agreement and this DPA.

Supplier shall notify Customer immediately if, in its opinion, an instruction infringes any Data Protection Laws.

3.5 Joint Controllers. To the extent that Supplier collects personal data directly from Data Subjects who are employees or contractors of the Customer in the course of providing the Services described in the Agreement, as described in Supplier's privacy notices (http://www.mediaocean.com/privacy-policy) (for example customer issue tickets or training requests), Supplier is Controller of such information and is responsible for notifying Customer's staff of such personal data collection and processing. Customer may request reasonable access to personal data about its staff collected by Supplier (for example records of training completion). In this case Customer shall be deemed to be acting as Joint Controller with Supplier and shall be responsible for:

a notifying Customer's staff about the collection, processing and use of said Personal Data, and

b implementing technical and organisational measures designed to protect the Personal Data which has been transferred to them by the Supplier from accidental or unlawful destruction, loss, alteration, unauthorised disclosure, access or use.

4 Security of Personal Data

4.1 Security. Supplier shall implement, at its own cost and expense, appropriate technical and organisational measures designed to protect the Personal Data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure, access or use (each a "Security Incident") and in accordance with Supplier's security standards as set forth in the Agreement. These measures shall be of a standard no less than the standards compliant with good industry practice for the protection of personal data and of at least the minimum standard required by the Data Protection Laws.

4.2 Supplier Personnel. Supplier shall take reasonable steps to ensure that only authorised personnel have access to Personal Data and to limit access to Personal Data to only those employees that require access to perform their roles and responsibilities in connection with the Services. Supplier shall take reasonable steps to ensure that any persons whom it authorises to have access to the Personal Data including employees, agents and contractors:

(i) receive appropriate training regarding their responsibilities and obligations with respect to the processing, protection and confidentiality of Personal Data.

(ii) are subject to a duty of confidentiality (whether a contractual or statutory duty) that shall survive termination of their employment and/or contractual relationship.

4.3 Deletion or Return of Customer Data. Upon termination or expiration of the Agreement, Supplier shall, in accordance with the terms of the Agreement, delete or make available to

Customer for retrieval all relevant Personal Data in Supplier's possession, save to the extent that Supplier is required by any applicable law to retain some or all of the Personal Data. In such event, Supplier shall extend the protections of the Agreement and this DPA to such Personal Data and limit any further processing of such Personal Data to only those limited purposes that require the retention, for so long as Supplier maintains the Personal Data. At Customer's request, Supplier shall provider Customer with certificate of destruction and a written log evidencing any retention of Personal Data.

4.4 Security Incidents. Upon becoming aware of a Security Incident, Supplier shall notify Customer without undue delay and pursuant to the terms of the Agreement, but within no more than seventy two (72) hours, and shall provide such timely information as the Customer may reasonably require to enable Customer to fulfil any data breach reporting obligations under Data Protection Laws. Supplier will take steps to immediately identify and remediate the cause of such Security Incident. If a Security Incident requires notice to any regulator, data subject, or other third party, Customer shall have sole control over the content, timing, and method of distribution of any needed notice, unless otherwise required by applicable law. Customer shall reimburse Supplier all reasonable expenses incurred by Supplier in connection with any notice with respect to any breach of security or confidentiality for which Customer is wholly or partially responsible.

4.5 Indemnification. In addition to the terms set forth in the Main Agreement(s), Supplier agrees to fully indemnify, defend and hold harmless Customer, its directors, officers, employees and agents from and against any and all losses, damages, fees and expenses arising from any claims due to, arising out of, or relating in any way to Supplier's loss, alteration, or misuse of Personal Data, or unauthorised access to or destruction or disclosure of Personal Data.

5 Sub-processing

5.1 Sub-processors. The Customer authorises Supplier to engage the Sub-processors listed in Annex 3 to Attachment 1 to process the Personal Data in accordance with the Processing Instructions. Supplier shall keep a written record of all Sub-processors and shall, on request, make a copy of this record available to the Customer. Supplier shall remain fully liable to the Customer for the Sub-processor's performance, as well as for any acts or omissions of the Sub-processor as regards its processing of Client Personal Data.

5.2 Contracts with Sub-processors. Supplier shall ensure, before any processing of Personal Data takes place, that the Sub-processor is contractually bound to terms that are no less restrictive and at least equally protective of Personal Data as those imposed on Supplier under this DPA (including in relation to providing such access and assistance as the Customer requires from time to time). Supplier shall provide copies of documentation to evidence its compliance with this clause to the Customer promptly on request.

5.3 Changes to Sub-processors. Supplier may, by giving no less than thirty (30) calendar days' notice to Customer, add or make changes to the Sub-processors. The Sub-processors currently engaged by Supplier are listed at the Supplier's Vendor Management Policy page https://support-uk.mediaocean.com/hc/en-gb/articles/360000133347-Mediaocean-vendor-management-policy. The Vendor Management Policy page shall include a mechanism for Customer to subscribe to notifications of any new Sub-processors or changes to the Sub-processor list. Customer is responsible for ensuring that they subscribe to such notifications. Customer may object to the appointment of an additional or replacement Sub-processor within ten (10) calendar days of such notice on reasonable grounds relating to the protection of Personal Data, in which case Supplier shall have the right to cure the objection through one of the following options:

a Supplier will cancel its plans to use the Sub-processor with regard to Personal Data or will offer an alternative to provide the Services without such Sub-processor; or

b Supplier will take corrective steps requested by the Customer in its objection (which remove Customer's objection) and proceed to use the Sub-processor with regard to Personal Data; or

c Supplier may cease to provide or Customer may agree not to use (temporarily or permanently) the Services which would involve the use of such Sub-processor with regard to Personal Data, subject to a mutual agreement of the parties to reduce the remuneration for the Services considering the reduced scope of the Services.

If none of the above options are reasonably available and the objection has not been resolved to the mutual satisfaction of the parties within thirty (30) calendar days after Supplier's receipt of Customer's objection, either party may terminate the Agreement and Customer will be entitled to a pro-rata refund for prepaid fees for Services not performed as of the date of termination.

5.4 Emergency replacement. Supplier may replace a Sub-processor if the reason for the change is beyond Supplier's reasonable control. In such instance, Supplier will notify Customer of the replacement as soon as reasonably practical, and Customer shall retain the right to object to replacement Sub-processor pursuant to Section 5.2 above.

5.5 Transfers of Personal Data outside the EU/EEA. Supplier shall ensure that any transfer of Personal Data outside the EU is carried out in compliance with the Data Protection Laws. The EU SCCs as set out at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en#ntc12-L_2021199EN.01003701-E0012 will apply to Customer Data that is transferred outside the European Economic Area (EEA), either directly or via onward transfer, to any country not recognized by the European Commission as an Adequate Country. Supplier shall ensure that other appropriate safeguards are in place, for example binding corporate rules in accordance with Article 47 of the GDPR or standard data protection clauses adopted by the Commission. The SCCs will not apply to Customer Data that is not transferred, either directly or via onward transfer, outside the EEA. In relation to Personal Data that is protected by the EU GDPR, the EU SCCs (set out in Attachment 1) will apply completed as follows:

a Module 2 will apply;

b in Clause 7, the optional docking clause will apply;

c Customer may exercise its right of audit under clause 8.9 of the SCCs as set out in, and subject to the requirements of, clause 7.1 of this DPA;

d in Clause 9, Option 2 (General Written Authorization) will apply, subject to the requirements of clause 5 of this DPA, and the time period for prior notice of subprocessor changes shall be thirty (30) days;

e in Clause 11, the optional language will not apply;

f in Clause 17, Option 1 will apply, and the EU SCCs will be governed by ___ law;

g in Clause 18(b), disputes shall be resolved before the courts of ___;

h Annex I of the EU SCCs shall be deemed completed with the information set out in Annex I(a), Annex I(b), and Annex I(c) attached hereto;

i Annex II of the EU SCCs shall be deemed completed with the information set out in Annex II attached hereto; and

j Annex III of the EU SCCs shall be deemed completed with the information set out in Annex III attached hereto.

In the event that any provision of this DPA contradicts, directly or indirectly, the EU SCCs, the EU SCCs shall prevail.

5.6 Transfers of Personal Data outside the UK. Supplier shall ensure that any transfer of Personal Data outside the UK is carried out in compliance with the UK General Data Protection Regulation (UK GDPR) and any other applicable Data Protection Laws. The SCCs and the UK Addendum will apply to Customer Data that is transferred outside the UK, either directly or via onward transfer, to any country not granted an adequacy decision. Neither the SCCs nor the UK Addendum will apply to Customer Data that is not transferred, either directly or via onward transfer, outside the UK.

5.7 Transfers of Personal Data outside Switzerland. The Parties agree that transfers from Switzerland are made pursuant to the EU SCCs with the following modifications:

a The terms "General Data Protection Regulation" or "Regulation (EU) 2016/679" as utilised in the EU SCCs shall be interpreted to include the Federal Act on Data Protection of 19 June 1992 (the "FADP," and as revised as of 25 September 2020, the "Revised FADP") with respect to data transfers subject to the FADP.

b The terms of the EU SCCs shall be interpreted to protect the data of legal entities until the effective date of the Revised FADP.

c Clause 13 of the EU SCCs is modified to provide that the Federal Data Protection and Information Commissioner ("FDPIC") of Switzerland and shall have authority over data transfers governed by the FADP and the appropriate EU supervisory authority over data transfers governed by the GDPR. Subject to the foregoing, all other requirements of Section 13 shall be observed.

d The term "EU Member State" as utilised in the EU SCCs shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from exercising their rights in their place of habitual residence in accordance with Clause 18(c) of the EU SCCs.

6 Cooperation

6.1 Data Subjects' rights. Supplier shall provide commercially reasonable assistance, including by appropriate technical and organisational measures as reasonably practical, to enable Customer to respond to any inquiry, communication or request from a Data Subject seeking to exercise his or her rights under Data Protection Laws, including rights of access, correction, restriction, objection, erasure or data portability, as applicable. In the event such inquiry, communication or request is made directly to Supplier, Supplier shall promptly inform Customer by providing the full details of the request. For avoidance of doubt, Customer is responsible for responding to Data Subject requests for access, correction, restriction, objection, erasure or data portability of that Data Subject's Personal Data.

6.2 Data Protection Impact Assessments and Prior Consultation. Supplier shall, to the extent required by Data Protection Laws, provide Customer with reasonable assistance with data protection impact assessments or prior consultations with data protection authorities that Customer is required to carry out.

7 Security Reports and Audits

7.1 Security Reports. Supplier will make available to Customer all information necessary to demonstrate compliance with requirements of the Data Protection Laws and allow for and

contribute to audits, including inspections, conducted by the Customer or Customer's designated representative.

7.2 Audits. No more than once per year, Customer shall have the right to Audit Supplier's data privacy compliance upon written request. The Parties shall bear their own costs in connection with activities under this paragraph, except that, in the event that Customer requests onsite validation, Supplier has not disclosed a security incident, and Customer does not have a reasonable suspicion that Supplier has had a security incident, Supplier may charge a reasonable fee for assistance provided to allow for such onsite validation. If such onsite validation reveals material non-compliance with their obligations under this clause, however, then Customer shall not be responsible to the Supplier for any such fees. Moreover, Supplier will provide Customer with annual SOC2 Type II report as evidence of its compliance with the Data Protection Laws and this DPA. Any provision of security attestation reports (such as SOC2, Type II or equivalent report) or audits shall take place in accordance with Customer's rights under the Agreement.

8 Miscellaneous

8.1 Except as amended by this DPA, the Agreement will remain in full force and effect.

8.2 If there is a conflict between the Agreement and this DPA, the terms of this DPA will take precedence.

8.3 Any claims brought under this DPA shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement.

8.4 The applicable law and jurisdiction as set forth in the Agreement apply to this DPA.

ACCEPTED AND AGREED TO:

For the Customer:	For the Supplier:
	Mediaocean LLC
(Insert legal name of Customer)	
By:	By:
(Authorised Signature)	(Authorised Signature)
Print name:	Print name:
Title:	Title:
Date:	Date:

ANNEX IA: 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]

Name: _____

Address: _____

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

_____

Activities relevant to the data transferred under these Clauses: As described in Annex 1B

Role (controller/processor): Controller

Signature and date: _____

Data importer(s):

Name: Mediaocean LLC

Address: 120 Broadway, New York, NY 10271, United States

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

Nick Galassi, Co-founder and CFO, Mediaocean LLC (ngalassi@mediaocean.com)

Activities relevant to the data transferred under these Clauses: As described in Annex 1B

Role (controller/processor): Processor

Signature and date: ...

ANNEX IB: DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

The data subjects are employees of the data exporter, and if applicable of its customers and vendors.

Categories of personal data transferred

- User authentication details
- Business contact information
- Logs of actions taken by users within the system

Please note that no transfer of sensitive data is anticipated.

Frequency of transfer

Data will be transferred on a continuous basis.

Nature of the processing

Data importer will record, organise, store, retrieve and disclose the personal data as instructed by the data exporter.

Purpose(s) of the data transfer and further processing

Data importer will record, organise, store, retrieve and disclose the personal data as instructed by the data exporter.

The period for which the personal data will be retained

Customer will determine retention of the personal data within production systems. Supplier will further retain back-ups in line with Supplier's data retention policy which is designed to ensure that Supplier meets contractual and regulatory retention requirements.

ANNEX IC: COMPETENT SUPERVISORY AUTHORITY

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

CNIL

Commission Nationale de l'Informatique et des Libertés

3 Place de Fontenoy

TSA 80715

75334 PARIS CEDEX 07

France

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.

Mediaocean's security program is aligned with ISO27001 for Information Security and covers control areas including:

- Logical and physical access
- Network security
- Change control over application software development and over operational infrastructure
- Processing integrity
- Availability, resilience and data retention
- Incident management and response
- Risk management
- Vendor / third-party security assessment and risk management

Please see details below.

Mediaocean's security controls are inspected by an independent auditor. Annual SOC1 (SSAE18 / ISAE3402) and SOC2 Type 2 reports (covering Security, Confidentiality, Availability, Processing Integrity & Privacy) provide independent assurance of the design and effectiveness of our security.

The data importers may appoint processors as described in the vendor management policy.

Logical access

Access to in scope applications and systems is enforced through role-based logical access control mechanisms. Mediaocean has implemented a range of access controls to manage access by Mediaocean employees and contractors to clients' systems and data:

- Access to in scope applications and systems is restricted through the use of identification and authentication mechanisms, including the use of user IDs assigned to users.
- IT systems security for Mediaocean staff access is managed and administered by security administrators, and access to modify security configurations is restricted to appropriate personnel.
- Security administrators are notified of new hires requiring access to the network, including remote access, by People & Culture via ticket. Mediaocean user accounts are updated by the security administrators to reflect the changes as per the notification.
- Requests for material changes in access permissions to in scope systems and supporting infrastructure follow an established process, are documented in the appropriate system, and approved by authorized personnel prior to provisioning or deprovisioning. (Material changes are changes which grant or remove read or write access to customer data in customer facing applications or their supporting infrastructure)
- Security administrators terminate network access, including remote access, for Mediaocean staff members who leave the company within 2 business days of their leave date. Access is removed for our client facing applications or for the system resources they run on when staff no longer require access, including when they change roles or leave the company.
- Password rules are configured for accounts used by Mediaocean staff to the corporate network and to in scope applications and supporting infrastructure, in accordance with company standards..
- Mediaocean user access privileges are reviewed at least annually by the respective data owners for completeness and accuracy. Security groups with privileged access are reviewed quarterly. Inappropriate access is identified by the data owners and is removed by appropriate security administrators.

- Mediaocean requires the use of two-factor authentication for employees connecting remotely to the Mediaocean corporate network.

Physical security

At our data centers

All application suites except AV are hosted in co-location facilities or at a cloud service provider. To ensure acceptable minimum provisions for physical security at these sites, Mediaocean has put in place a vendor management policy which defines security, confidentiality, and privacy requirements by vendor class. Mediaocean maintains contractual relationships with all vendors which define the required security, confidentiality, and privacy commitments, as applicable, for all relevant parties. Mediaocean performs security reviews in line with the requirements of the vendor management policy when onboarding a new vendor, and periodically in line with the requirements of the vendor management policy to ensure adherence to stipulated requirements.

All data centers and cloud hosting facilities that Mediaocean uses to host production services must meet requirements in relation to physical security, access control, human resources security, incident management and, where applicable, handling of personal data.

At our offices

The Louisville data center, which hosts AV, is operated by Mediaocean at its office premises. Physical security controls at our offices include the following:

- Physical access to Mediaocean premises which house IT assets is restricted to appropriate personnel by an integrated key card access system.
- IT assets are stored in a secured area and access is restricted to appropriate IT Operations personnel. Data centers and other secure areas are set up as separate zones in the access card system. Access to secure areas must be authorized by the manager responsible for that zone – this can either be granted by job function or on an individual basis. Additional security measures (e.g. intruder alarms, CCTV, security staff) are implemented in accordance with local risk assessments.
- Environmental and power failure safeguards are in place at data centers to protect IT assets.
- Access to modify user permissions in the integrated key card access systems is restricted to appropriate personnel.
- Facilities administrators are notified of changes to physical access to the data center for new hires, terminations, and transferred employees by People & Culture via ticket. Key card access to the data center is updated by the Facilities administrators to reflect the changes as per the notification. Employees are given an access card for the office to which they are assigned. Visitors from other Mediaocean offices may additionally be given an access card, and other visitors are given temporary passes.
- Physical access privileges are reviewed at least annually by the respective zone owners for completeness and accuracy. Physical access privileges for high security areas are reviewed quarterly. Inappropriate access is identified by the zone owners and is removed by appropriate administrators.

Network security

Secure Transport or Encryption technologies (i.e. VPN, Citrix, SSL, TLS, HTTPS) are implemented for points of connectivity and to protect the in scope systems and data in transit on at risk networks. These methods protect data in transit from interception by unauthorized third parties. Network security controls include the following:

- Mediaocean production systems are protected by dedicated network infrastructure including firewalls. Mediaocean maintains a segmented network with separate vlans for dedicated purposes.
- Firewall rules are in place to ensure all external connections to Mediaocean's network pass through a firewall.

- Mediaocean uses continuous monitoring solutions to identify and notify appropriate resources of potential or actual security or system failures and for performance and capacity issues. Thresholds are configured to trigger different levels of alert severity based on the criticality of the issue.
- Firewall tools are configured to send alerts to IT Operations personnel summarizing activity, including potential security breaches and other security incidents.

Endpoint protection including antivirus is deployed to all user endpoints. The vendor operates a security operations control center and notifies IT Operations of potential issues. IT Operations follows up to research and resolve the incident. Mediaocean encrypts company issued user laptops.

Change control

Mediaocean has adopted standardized change management controls which are followed for changes to in-scope systems and their supporting infrastructure, including the following:

- Adopted change requests are transitioned through the workflow and documented in a ticket.
- For each change, appropriate staff determine and execute an overall Quality Assurance test plan.
- Adopted change requests follow the approval workflow prior to deployment or implementation.
- Emergency changes that require deviations from standard procedures are documented and evaluated on a case by case basis by appropriate personnel.
- Segregation of duties is enforced throughout the change management process by clearly defining responsibilities and permissions for each party within the change management lifecycle.
- Planned changes to system components are communicated to internal users via standard communication channels.
- Relevant changes are communicated to external users by posting notices on the externally accessible ticketing system portal and automated email alerts, if the external user subscribes to the alerts.

Applications software

Mediaocean has adopted a formal systems development life cycle (SDLC) methodology that governs the development, acquisition, implementation, and maintenance of systems and applications, including a formal change management methodology that governs the request, approval, testing, and promotion of changes into production for the in scope applications, databases and related technology. This is a customized methodology which uses features from agile development and from more traditional, waterfall development approaches.

Each development team has a defined development process starting with project initiation and ending with release & implementation. The process is followed consistently for the team's projects and ensures that key control activities are performed for each project. Different development teams implement tools and processes which are appropriate for the development platform they are using.

The processes are scalable for different types of project. For example, more detailed functional requirements (or user stories) and technical designs are required for the development of a new product than for a minor modification to an existing project. However, in all cases the key controls are the same in terms of approval, testing and authorization for deployment. Additionally:

- Separate development, testing, and production environments are in place.
- Source code is stored and managed via the agreed upon source control software for the platform.
- Defects are tracked and categorized by the project team. Critical defects are resolved by Development personnel and retested by QA personnel, prior to releasing modifications into the production environment.
- Software configuration standards and technical requirements are documented in a shared knowledge-base repository.
- Software engineers undergo annual training on secure coding best practices.

Operational infrastructure

Mediaocean maintains standard image templates that are utilized when building new production systems, for applicable systems. For other systems, operations teams follow a documented process to standardize installation of new services. Other standardized system hardening practices that have been implemented include: restricting protocol access, removing or disabling unnecessary software, network ports and services, removing unnecessary files, user accounts, restricting file permissions, patch management and logging.

A patch management process has been implemented to monitor and deploy critical system security updates released by the vendor. Mediaocean aims to put in place a remediation plan for any critical vulnerabilities of which we become aware in order to remediate the issue within 30 days. A critical severity is assigned to any reported 3rd party critical vulnerability that applies to our services based on the use of and data involved with the 3rd party software, if the confidentiality or integrity of data is endangered. For lower priority vulnerabilities, the IT Operations team will liaise with the Product and Engineering team in order to coordinate the remediation plan within the application release schedule. Quarterly patch reviews include checks to identify any out of support software or hardware.

Processing integrity

Mediaocean ensures the accuracy and integrity of the client data we process through various mechanisms, establishing that data are complete, valid, accurate, and authorised. Processing integrity procedures are documented and are made available to personnel. Controls include the following:

- Field inputs are validated for compliance with defined input requirements.
- Mediaocean client production environments are either single-tenant environments, or else in the case of multi-tenant environments are logically separated to ensure that client users are only able to access their own organization's data.
- In scope systems generate and retain application error logs or similar discrepancy reports to facilitate troubleshooting. For applicable systems, such logs generate notifications to alert appropriate personnel of potential erroneous data entered by an end-user.
- Application logs are generated and retained to track actions by users and administrators of the systems.
- For mainframe systems, production processing jobs are scheduled through automated tools and are monitored by Mainframe Operations personnel for issues in processing and abnormalities. Production job scheduling changes are documented in a ticketing system and are implemented by appropriate Mainframe Operations personnel.
- Abnormalities that require action are tracked in a ticketing system, investigated, and resolved by Mainframe Operations personnel
- Mediaocean has a documented data maintenance policy that governs the process for making client production data additions, changes, and deletions, and includes a requirement for authorizations by approved client contacts prior to performing and changes. Customer Experience Administration personnel conduct a quarterly review to confirm with account teams that Authorized Client Approver lists are up to date. Any identified changes to the Authorized Client Approver list and/or Customer Experience portal access are updated appropriately.

Availability, resilience and data retention

The objectives of Mediaocean's data retention policies are to

- Provide and retain a copy of all production data, software and systems so as to allow recovery from processing interruptions, as described in the Mediaocean Business Continuity Plan.
- Retain data in the event of inadvertent deletion or corruption. Requirements for data retention are defined in Mediaocean's internal Data Classification and Data Retention policies.
- Meet statutory requirements for retention of historical records.

Requirements for data retention are defined in the Data Classification policy and in the Data Retention policy. Data retention controls include the following:

- Critical client facing systems are configured for high availability.

- Data for in scope systems is encrypted at rest using encrypted storage. Data is replicated to geographically separate failover sites to allow for system operation in the event of a system or data center failure.
- Backups are managed using automated scheduling tools configured by authorized personnel. Backup scheduling change requests are documented in a ticketing system and must be approved by appropriate IT Operations managers.
- IT Operations personnel monitor backups for abnormalities. Abnormalities that require action are tracked in a ticketing system, investigated, and resolved by IT Operations personnel.
- Backups are stored off-site based on data retention and restoration policies and procedures. Access to offline storage, backup data, systems, and media is restricted to IT Operations personnel through the use of physical and logical access controls. Backups are retained encrypted in cloud storage.
- Disaster recovery and contingency plans are in place and are validated on an annual basis. A recovery test is performed at least annually by Mediaocean personnel to ensure that a full system recovery can be performed completely and accurately.
- IT Operations personnel verify ability to recover data from backups by performing restores. Restores are performed as needed and at least quarterly. Restore requests are documented in a ticketing system and are performed by IT Operations personnel.
- IT Operations use appropriate information to assess the requirement to add capacity and address issues in accordance with defined change control procedures.
- IT Operations managers continuously track all critical system outage alerts to resolution through JIRA tickets.

When data has passed its retention period, company procedures for secure disposal must be followed when disposing of any equipment capable of storing information. Company policies require employees to use secure confidential waste bins or shredders for the disposal of any physical confidential documents. Confidential waste bins are locked and transported to a shredding facility by a third party.

Incident management and response

There is a documented & approved plan for handling security, confidentiality, processing integrity, availability, and privacy incidents. Mediaocean classifies security incidents including data & policy breaches, technology issues and availability incidents and documents procedures for handling them. Mediaocean publishes instructions to personnel explaining how to report potential & actual incidents, and also to customers explaining how to report issues including support requests and security incidents. External users are informed about the ticket portal when they receive training on Mediaocean applications. Also, external users are directed from the Mediaocean web site (www.mediaocean.com – Customer Experience tab) to the ticketing system, where they can raise a support ticket or chat with the Customer Experience Group during business hours. Phone numbers and email addresses are also made available to clients to enable them to contact the Customer Experience team, and Mediaocean web applications include an in-application chat option as well.

Controls around incident management include the following:

- Incidents are documented in tickets which are assigned to appropriate personnel and closed following resolution.
- Mediaocean publishes communications plans for notifying relevant personnel and affected users about incidents.
- Incidents are reviewed as needed for lessons learned, to identify recommendations on the reduction of the risk recurrence.
- Client support issues are documented, classified and communicated to the appropriate department for resolution.
- Service levels, including clients' contractual SLAs, are configured into the client support issue tracking system to ensure that Customer Experience team members are aware of performance goals. The issue tracking system issues notifications to Customer Experience team members and to Customer Experience management in the event that service levels are breached.

Privacy

In the course of, and ancillary to, our business activities, Mediaocean collects, stores and processes data, including Personal Information and Sensitive Personal Information (also known as Special Categories of Data). We recognize the importance of protecting Personal Information and have implemented a Privacy Policy to ensure that it is collected, stored, and processed properly and in accordance with applicable laws and regulations, so as to protect the confidentiality, integrity and availability of the Personal Information.

- Mediaocean's privacy commitments and associated system requirements are communicated to internal users by the Privacy Policy which is made available to internal personnel on the Company Intranet.
- Information about Mediaocean's privacy practices is documented and made available to appropriate external users on the Customer Experience portal and via a link that is automatically included in emails from the portal.
- Mediaocean maintains a register of personal data processing, which outlines the Company's legal basis for processing data and for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information. The register is reviewed on a quarterly basis by the Information Security & Compliance team.
- Upon the introduction of a new or changed procedure that involves the handling of personal data, the register of personal data processing is updated and a data protection impact assessment ("DPIA") is performed.
- In cases where personal data is processed on the basis of Mediaocean's legitimate interests, and where the Privacy team has concerns that the company's interests are overridden by the rights of the data subject, the Privacy team performs an additional Legitimate Interests Assessment.
- In cases where new or changed procedures require the transfer of personal data outside the EU, the Privacy team performs an additional Transfer Impact Assessment.
- Mediaocean has procedures in place to notify and obtain explicit consent from clients if information that was previously collected is to be used for purposes not previously identified in the privacy notice.
- Mediaocean has put in place policies and procedures to handle Data Subject Access Requests (DSARs), including requests for access to view personal information and requests for deletion of personal information. DSARs are documented, classified and escalated to the appropriate department for resolution. Resolution is communicated to external users via the Customer Experience portal.
- Mediaocean maintains a list of vendors to whom disclosures of personal information are authorized. Service providers with access to personal information are required to sign an agreement which stipulates the required privacy commitments. Adherence to these commitments is monitored using the procedures described in the section on Physical security above.
- Mediaocean's contracts with clients stipulate the required security and privacy commitments and define the parties' rights in respect of data processed within hosted solutions.
- Mediaocean has put in place policies and procedures to address the misuse of personal information which includes documented, classification, escalation and communication to appropriate internal and external parties. Instances of noncompliance with objectives related to privacy are documented, reported, and corrected as necessary.

Additional control areas

People & Culture

The People & Culture team has implemented policies and procedures to ensure that:

- Mediaocean staff are qualified to do the jobs they are hired to do.
    - Hiring procedures include a comprehensive screening of candidates for key positions and consideration of whether the verified credentials are commensurate with the proposed position.

- Background investigations are initiated prior to new hire, for all offices other than India. For employees in the India office, background investigations are initiated within one week of hired date.
- Written job descriptions specifying the responsibilities for the role are prepared when positions below executive level are advertised..

- They have the training and knowledge to do their jobs in accordance with company requirements.
  - The Learning team oversees the development and publication of on-line learning courses covering industry knowledge topics, knowledge of Mediaocean applications, use of internal tools and systems, management skills and HR, ethics and compliance. The Learning team publishes and assigns courses and tracks attendance.
  - The security, confidentiality, availability and privacy obligations of users and Mediaocean's security commitments to users are communicated to new hires and contractors during new hire orientation. New hires and contractors are required by People & Culture to read and acknowledge receipt of the Information Security policy upon commencement of employment.
  - The responsibilities of Mediaocean employees and contractors, including security, availability, processing integrity and confidentiality commitments and associated system requirements, are communicated through the Information Security Policy and other policy and procedure documents published on the Company Intranet.
  - Annual information security refresher training, including a module related to privacy, is completed by all employees below senior executive level.
  - Continuous feedback goals are completed by all employees below senior executive level and the employee's manager.
- They adhere to codes of conduct for ethical behaviour.
  - People & Culture publish an Employee Handbook detailing conduct standards. The Handbook includes information about reporting mechanisms in place for reporting incidents and compliance concerns anonymously.
  - A formal disciplinary process, up to and including termination, has been documented to help ensure the correct and fair treatment for employees who are suspected of committing breaches of information security or privacy policies or failing to adhere to conduct standards.
  - New hires and contractors are required by HR to sign a non-disclosure agreement upon commencement of employment.

Other organisational controls

- Mediaocean documents security policies and procedures which have been implemented in order to meet the organization's objectives for security, availability, confidentiality, processing integrity and privacy. Responsibility and accountability for designing, developing, implementing, operating, monitoring, maintaining, and approving security policies is shared across management and is documented within each document. Security policies are reviewed and approved on at least an annual basis by designated personnel noted in the Responsibility section of each policy and procedure document. Security policies are made available to internal personnel on the Company Intranet.
- Mediaocean identifies threats to the security, availability, processing integrity, confidentiality, and privacy of systems and data on an ongoing basis, and records identified risks in a Risk Register and assigns a severity in terms of quality and continuity of service, regulatory and reputational impact and potential financial loss. Information Security works with process owners to identify treatments to identified risks. Risk treatments are evaluated on a quarterly basis, and are formally assessed and documented on the Risk Register. An annual Risk report is prepared and reviewed by the Information Security & Compliance team and communicated to senior management.
- Mediaocean establishes an internal audit charter annually to guide the activities of the Internal Audit team. The Internal Audit team conducts internal audit testing quarterly and documents findings in an audit report. Internal audit findings are reported back to the department managers responsible for the controls. An annual report of Internal Audit findings is prepared by the Information Security & Compliance team and shared with senior management.

- The Security & Compliance team conducts internal vulnerability scans, at least quarterly. Results are reviewed and any issues identified are researched and resolved as part of the patching and/or incident change management. External Penetration testing for web-based applications is performed annually to identify security weaknesses and vulnerabilities. Any identified vulnerabilities are risk assessed and remediation plans are implemented appropriately.
- IT Operations and Information Security teams subscribe to and monitor external sources to identify technological changes, security vulnerabilities, and privacy updates and assess their effect on internal systems.
- Mediaocean has implemented threat detection systems which monitor all traffic on the corporate network including traffic to production systems. Identified issues are reported to Operations and Security staff by the Security Operations Center vendor that provides 24/7 monitoring service, and are researched and resolved.
- Endpoint privilege management software is deployed to all user endpoints to ensure that only authorized software is installed on Mediaocean owned devices. Mobile device management software is deployed to ensure mobile device applications accessing Mediaocean email are authorized and secure. Email threat detection software has been implemented to detect advanced email threats and to block or quarantine suspect emails coming into the organization.
- Mediaocean obtains industry certifictions for applicable systems by undergoing annual auditing based upon an approved scope. Mediaocean obtains annual SOC1 and SOC2 (SSAE 18 / ISAE 3402) Type II reports.
- Mediaocean obtains cyber insurance to mitigate the financial risk of security incidents.

ANNEX III: LIST OF SUB-PROCESSORS

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

Provider	Location(s)	Service(s) supported
Data centers		
Amazon Web Services	Ireland, India, United States, Singapore	All except AV, Symsys
Kyndryl	New York, United States	Estimates and costs, Dealmaker, Global plans, Buyer and Seller workflow, DS, OX
Iron Mountain	Haarlem, Netherlands	Symsys
Maincubes	Amsterdam, Netherlands	Symsys
Mijnserver	B.V. Rotterdam, Netherlands	Symsys
Service Express	Middlesex, United Kingdom	Buyer and Seller workflow, DS
Off-site storage		
Amazon Web Services	United States	All except AV, Symsys
Iron Mountain	Kentucky, Illinois & New York, United States	AV, OX
Vital Records	New Jersey, United States	Estimates and costs, Buyer and Seller workflow, DS
Data warehouses		
Snowflake	United States	Business Intelligence
Sisense	United States	Business Analytics
Outsourced support		
Microsourcing	Philippines	All
QBurst	India	Buyer workflow (Prisma development)
Wideout	Philippines	Global plans (implementation)
Ancillary services		
New Relic	Server Central data center in Illinois, United States	Estimates and costs, Media finance, Global plans, Buyer and Seller workflow
Pendo	Google Cloud Platform data centers in the United States	Estimates and costs, Media finance, Global plans, Buyer and Seller workflow

The list of sub-processors is maintained at https://support-na.mediaocean.com/hc/en-us/sections/360009114773-Vendor-Management.

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

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

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

Part 1: Tables

Table 1: Parties

Start date		
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' details	Full legal name: Trading name (if different): Main address (if a company registered address): Official registration number (if any) (company number or similar identifier):	Full legal name: Mediaocean LLC Main address: 120 Broadway, New York, NY 10271, United States Official registration number (if any) (company number or similar identifier):
Key Contact	Full Name (optional): Job Title: Contact details including email:	Full Name (optional): Nick Galassi Job Title: Co-founder and CFO Contact details including email: ngalassi@mediaocean.com
Signature (if required for the purposes of Section 2)		

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: 4 June 2021 Reference (if any): 2021/914/EU Other identifier (if any): See link

Table 3: Appendix Information

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

Annex 1A: List of Parties:
Annex 1B: Description of Transfer:
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:
Annex III: List of Sub processors (Modules 2 and 3 only):

Table 4: Ending this Addendum when the Approved Addendum Changes

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

Part 2: Mandatory Clauses

Entering into this Addendum

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

Interpretation of this Addendum

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

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.

Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

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

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

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

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

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

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

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

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

Incorporation of and changes to the EU SCCs

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

    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

    a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

    b. In Clause 2, delete the words:

        "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

c. Clause 6 (Description of the transfer(s)) is replaced with:

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

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

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

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

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

f. References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

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

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

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

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

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

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

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

m. Clause 17 is replaced with:

> "These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

> "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data

exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

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

Amendments to this Addendum

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

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

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

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

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

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

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

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

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

Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.