DATA PROTECTION AND INFORMATION SECURITY ADDENDUM

Approved for Use – March 2026

This agreement consists of 26 pages including this one. It contains technical and organizational measures for data security and the European Commission's Standard Contractual Clauses (SCCs) to comply with the terms of GDPR Article 46(2)(c) and (d).

Via Agostino Bertani 6

20154 Milan, Italy

Tel. +39.028.725.9395

This Data Protection and Information Security Addendum (this "Addendum") forms part of the terms of service (the "Agreement") for the Client's purchase of services (identified either as "Services" or otherwise in the applicable agreement, and hereinafter defined as "Services") from CoreView S.r.l. or its Affiliates ("CoreView") to reflect the parties' agreement about the Processing of Personal Data. This Addendum includes by reference the terms and conditions of the Agreement. In the event of any inconsistencies between this Addendum and the Agreement, the parties agree that the terms and conditions of the Addendum will control. In the event of conflict between this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail only insofar as they are applicable to a transfer of Personal Data.

Throughout the term of the Agreement and for as long as CoreView controls, possesses, stores, transmits, or processes Personal Data as part of the Services and until such time as all Personal Data have been expunged from CoreView's systems and possession post termination of the Services, CoreView and Client will comply with the requirements set forth in this Addendum.

1. Definitions

Capitalized terms herein shall have the definition ascribed in the Agreement. Capitalized terms not otherwise defined have the meanings set forth in this section:

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity, where "control" refers to the power to direct or cause the direction of the subject entity, whether through ownership of voting securities, by contract or otherwise.

"Authorized Personnel" means CoreView's and its Affiliate's employees or subcontractors who: (i) have a need to receive or access Personal Data to enable CoreView to perform its obligations under the Agreement; and (ii) are bound with CoreView by confidentiality obligations sufficient for the protection of Personal Data in accordance with the terms and conditions set forth in the Agreement and this Addendum.

"Client" shall mean the legal entity purchasing the Services from CoreView and any applicable Affiliates.

"Common Software Vulnerabilities" (CSV) are application defects and errors that are commonly exploited in software. This includes but is not limited to: (i) The CWE/SANS Top 25 Programming Errors – see http://cwe.mitre.org/top25/ and http://www.sans.org/top25-software-errors/; (ii) The Open Web Application Security Project's (OWASP) "Top Ten Project" – see http://www.owasp.org

"Controller" means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

"Data Protection Laws" mean all applicable laws, standards, guidelines, policies, regulations, and procedures applicable to CoreView, including as a result of its provision of the Services to the Client and pertaining to data security, confidentiality, privacy, and breach notification. Data Protection Laws includes but is not limited to the EU General Data Protection Regulation 2016/679 ("GDPR"), as the same may be amended from time to time.

"EU/UK Data Protection Laws" means: (i) Regulation 2016/679 of the European Parliament and of the Council 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) (the "EU GDPR"); (ii) the EU GDPR as assimilated into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "UK GDPR"); (iii) the EU e-Privacy Directive (Directive 2002/58/EC); and (iv) any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (i), (ii) or (iii); in each case as may be amended or superseded from time to time

"Europe" means, for the purposes of this DPA, the European Union, the European Economic Area ("EEA") and/or their member states, Switzerland, and the United Kingdom.

“Industry Standards” mean generally recognized industry standards, best practices, and benchmarks.

“Non-EU Data Protection Laws” means any other applicable laws to the processing of Client’s Personal Data, including without limitation the California Consumer Privacy Act (“CCPA”); the Canadian Personal Information Protection and Electronic Documents Act (“PIPEDA”); and the Brazilian General Data Protection Law ("LGPD"), Federal Law no. 13,709/2018, and its implementing regulations.

“Personal Data” also known as Personally Identifiable Information (PII), is any information regarding Client customers, employees, or subcontractors held or accessed by CoreView that can be used on its own or combined with other information to identify, contact, or locate a natural person, or to identify an individual in context. Examples of Personal Data include first and last name, address, social security number or national identifier, biometric records, geolocation information, driver’s license number, account number or username with password or PIN, either alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc. Personal Data includes those data elements defined under applicable state or federal law in the event of a Security Incident.

"Process(ing)” means any operation or set of operations which is performed on personal data or on sets of personal data, whether by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction;

“Processor” means the natural or legal person, public authority, agency, or other body which processes personal data on behalf of the Controller.

“Regulator” means the data protection supervisory authority which has jurisdiction over a Controller’s Processing of Personal Data.

"Restricted Transfer" means: (i) where the EU GDPR applies, a transfer of personal data from the European Economic Area or Switzerland to a country outside of the European Economic Area or Switzerland which is not subject to an adequacy determination by the European Commission; and (ii) where the UK GDPR applies, a transfer of personal data from the United Kingdom to any other country which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018.

“Third Countries” means all countries outside of the scope of the Data Protection Laws of the European Union, the European Economic Area (“EEA”) or the United Kingdom, excluding countries recognized by the applicable Regulator as providing adequate protection for Personal Data from time to time.

“Security Incident” is any actual occurrence of: (i) unauthorized access, use, alteration, disclosure, loss, theft of, or destruction of Personal Data or the systems / storage media containing Personal Data; (ii) illicit or malicious code, phishing, spamming, spoofing; (iii) unauthorized use of, or unauthorized access to, CoreView’s systems; (iv) inability to access Personal Data or CoreView systems as a result of a Denial of Service (DOS) or Distributed Denial of Service (DDOS) attack; and (v) loss of Personal Data due to a breach of security; provided, however, Security Incidents do not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, or other network attacks on firewalls or networked systems.

“Security Vulnerability” is an application, operating system, or system flaw (including but not limited to associated process, computer, device, network, or software weakness) that can be exploited resulting in a Security Incident.

“Standard Contractual Clauses” means the standard contractual clauses for the transfer of Personal Data from the European Economic Area to parties established in third countries, as set out in the annex to Commission Decision 2021/914/EU (“EU SCCs”), the United Kingdom International Data Transfer Addendum to the EU Commission Standard Contractual Clauses version B1.0 (“UK IDTA”), and the EU SCCs as updated per the Swiss Federal Data Protection and Information Commissioner requirements set out in “The transfer

of personal data to a country with an inadequate level of data protection based on recognized standard contractual clauses and model contracts 27 August 2022" ("Switzerland Addendum"), each as updated from time to time. The Standard Contractual Clauses shall be incorporated by reference and form an integral part of this DPA.

"Supervisory Authority" means a public authority concerned with the protection of the rights and freedoms of natural persons impacted by the Processing of Personal Data.

Capitalized terms used in this Addendum shall have the same meaning given to them under Data Protection Laws or if not defined thereunder, the EU GDPR, unless a different meaning is specified herein. In regard to the CCPA, terms used in the applicable provisions of the DPA where the CCPA is the applicable law shall be replaced as follows: "Personal Data" shall mean "Personal Information"; "Controller" shall mean "Business"; "Processor" shall mean "Service Provider"; and "Data Subject" shall mean "Consumer".

2. Roles of the Parties and Compliance with Data Protection Laws

As between CoreView and Client, Client shall be the Controller and CoreView shall be the Processor with respect to the Processing of Client's Personal Data pursuant to this Addendum. CoreView acknowledges Client may be acting as a Processor to its Affiliates and those Affiliates as Processors to other third parties. Where such circumstances apply to the Personal Data Processed by CoreView, Client represents and warrants that it has the appropriate authority to engage CoreView as a subsequent Processor.

Each party shall comply with its obligations under all applicable Data Protection Laws. As such:

a) Client shall determine the scope, purpose, and manner in which such Personal Data may be processed by CoreView, and CoreView will limit its Processing of Personal Data to that which is instructed in the manner necessary to provide the Services, or otherwise to comply with applicable Data Protection Laws. In the event CoreView is subject to a legal requirement to process the Personal Data other than in accordance with the Controller's instructions, it shall notify the Controller of the requirement prior to Processing unless prohibited from doing so on the important grounds of public interest;

b) Unless you have specifically consented to us doing so, CoreView will not use Personal Data to train, refine or improve our Corey AI product or other Services. We may collect data about how users interact with and operate the Corey AI product and our Services, or we may deidentify certain information about your use of these services (collectively, "Usage Data"). Usage Data is necessary for us to be able to offer and provision the services, and to continue to improve and refine the Services, including Corey AI;

c) Client agrees that, without limitation of CoreView's obligations in this Addendum, Client is solely responsible for its use of the Services, including (a) making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of the Personal Data; (b) securing the account authentication credentials, systems, and devices Client uses to access the Services; (c) securing Client's systems and devices that CoreView uses to provide the Services; and (d) backing up Personal Data;

d) Client is solely responsible for evaluating for itself whether the Services, the security measures and CoreView's commitments under this Addendum will meet Client's needs, including with respect to any security obligations of Client under applicable Data Protection Laws or other laws. Client acknowledges and agrees that at the date of execution of this Addendum (considering the state of the art, the costs of implementation and the nature, scope, context and purposes of the Processing of Personal Data as well as the risks to individuals) the security measures implemented and

maintained by CoreView provide a level of security appropriate to the risk in respect of the Personal Data;

e) Client warrants that: (i) it has established or ensured that another party has established a legal basis for CoreView's Processing of Personal Data contemplated by this Addendum; and (ii) all notices have been given to, and necessary consents and rights have been obtained from, the relevant data subjects and any other party as may be required by Data Protection Laws and any other laws for such Processing;

f) CoreView will process Client Personal Data to the extent necessary to comply with other documented reasonable instructions provided by Client (e.g., via email) where such instructions are consistent with the terms of the Agreement and this Addendum. If an instruction provided by Client infringes the GDPR or other applicable Data Protection Laws, CoreView shall immediately inform Client.

g) CoreView shall implement the technical and organizational measures appropriate to the size and complexity of CoreView's operations and the nature and the scope of its activities and the Personal Data involved, to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure, or access, and against all other forms of unlawful Processing, including but not limited to unnecessary collection or further Processing. This Addendum includes a general description of such measures.

h) CoreView shall promptly notify Client if CoreView receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure, data portability, object to the Processing, or its right not to be subject to an automated individual decision making ("Data Subject Request"). Taking into account the nature of the Processing, CoreView shall assist Client by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Client's obligation to respond to a Data Subject Request under applicable Data Protection Laws. In addition, to the extent Client, in its use of the Services, does not have the ability to address a Data Subject Request, CoreView shall upon Client's request provide commercially reasonable efforts to assist Client in responding to such Data Subject Request, to the extent CoreView is legally permitted to do so and the response to such Data Subject Request is required under applicable Data Protection Laws. In the event that Client asks for assistance where CoreView has already made available to and made Client aware of functionality which would enable Client to fulfil the request without CoreView's assistance, Client shall be responsible for any reasonable costs arising from CoreView's provision of such assistance.

3. Information Security Technical and Organizational Measures:

CoreView's information security program includes, but is not limited to, the following elements:

3.1 Management Direction for Information Security.

a) **Security Policies and Standards**. CoreView maintains information security policies and standards that: (i) define the administrative, physical, and technological controls to protect the confidentiality, integrity, and availability of Personal Data, Client Data, and CoreView systems (including mobile devices and removable media) used to provide the Services to Client; (ii) encompass secure access, retention, and transport of Personal Data; (iii) provide for disciplinary or legal action in the event of violation of policy by employees or CoreView's subcontractors and vendors; (iv) prevent unauthorized access to Client Data and CoreView systems; (v) employ the requirements for assessment, monitoring and auditing procedures, and systems to ensure CoreView is compliant with the policies; and (vi) require the conduct of an annual assessment of the policies, and upon Client's written request, provide attestation of compliance.

b) **Monitoring and Enforcement.** CoreView monitors compliance with its privacy policies and procedures to address privacy related complaints and disputes.

c) **Independent Review of Information Security.** CoreView's approach to managing information security and the implementation of appropriate policies and procedures (i.e., control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur. Independent reviews may include internal auditors or third-party security or audit firms.

3.2 **ORGANIZATION OF INFORMATION SECURITY**

a) **Segregation of Responsibilities.** CoreView will ensure that the responsibilities of its personnel are appropriately segregated to reduce opportunities for unauthorized or unintentional access, modification or misuse of the organization's assets.

b) **Regulatory Contact**: If applicable to CoreView's business or required by law, CoreView will maintain contact with the governing regulatory authorities to ensure ongoing compliance with the mandated regulatory requirements.

3.3 **TELEWORKING**

a) **Teleworking Requirements.** If CoreView allows Authorized Personnel to work remotely in support of CoreView services, CoreView shall provide Authorized Personnel with one of the following technologies to mitigate the inherent security risks of remote access:

I. A CoreView provided and controlled device (e.g., laptop or workstation) that is securely managed by the CoreView's information technology team(s); OR

II. A secure technology, service, or platform, that enables the CoreView to manage the security configuration of personally owned devices used to provide CoreView services, in order to meet the security requirements of both CoreView and Client, as defined within this Addendum.

3.4 **HUMAN RESOURCES SECURITY**

a) **Screening.** Background verification checks on all candidates for employment is carried out in accordance with relevant laws, regulations, and ethics; and it is proportional to the business requirements, the classification of the Client information to be accessed and the perceived risks.

b) **Security and Privacy Training.** CoreView trains new and existing employees and subcontractors to comply with the data security and data privacy obligations under this Agreement and this Addendum. Ongoing training is to be provided at least annually.

c) **CoreView ensures** that its employees, contractors, other sub-contractors or vendors are required to sign a confidentiality or non-disclosure agreement to protect Client Personal Data.

d) **Termination or Change of Employment Responsibilities**. Information security responsibilities and duties that remain valid after change of employment shall be defined, communicated to the employee or contractor, and enforced.

3.5 **ASSET MANAGEMENT**

a) CoreView maintains an inventory of assets associated with information and information processing facilities.

b) Assets maintained in the inventory must be assigned to an individual or group that is accountable and responsible for the assigned asset(s).

c) Acceptable use of assets is defined within a formal policy or standard.

d) The return of assets is clearly communicated, via policies and/or training, to all employees and contractors upon termination of their employment, contract, or agreement. Return of assets shall be documented by CoreView.

e) CoreView classifies data in terms of legal requirements, value, criticality, and sensitivity to unauthorized disclosure or modification. Procedures for handling assets are developed and implemented in accordance with the information classification scheme adopted by the organization.

3.6 **MEDIA HANDLING**

a) Procedures must be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.

b) Upon expiration or termination of the Agreement or upon Client's written request, CoreView and its Authorized Personnel will promptly return to Client all Personal Data and/or securely destroy Client Personal Data. At a minimum, destruction of data activity is to be performed according to the standards enumerated by the National Institute of Standards, Guidelines for Media Sanitization - see http://csrc.nist.gov/. If destroyed, upon request, an officer of CoreView must certify to Client in writing within ten (10) business days of completed destruction that all Client Personal Data has been destroyed. If CoreView is required to retu any confidential information or metadata to comply with a legal requirement, CoreView shall provide notice to both the general notice contact in the Agreement as well as Client's designated Security Contact (if provided to CoreView).

3.7 **ACCESS CONTROL**

a) CoreView ensures that Personal Data are accessible only by Authorized Personnel after appropriate user authentication and access controls that satisfy the requirements of this Addendum.

b) Two-factor authentication is required for remote connectivity into CoreView systems or networks.

c) Each Authorized Personnel has unique access credentials and receives training which includes a prohibition on sharing access credentials with any other person.

d) CoreView has a formal user registration and de-registration process for enabling assignment of access rights.

e) CoreView has a formal user access provisioning process to assign or revoke access rights for all user types to all systems and services.

f) The allocation and use of privileged access rights is restricted and controlled.

g) User access rights must be reviewed at regular intervals but at a minimum on an annual basis.

h) The access rights of all employees and external party users to information and information processing facilities is removed upon termination of their employment, contract or agreement, or adjusted as appropriate upon change in role or responsibilities.

i) Password management systems is interactive and ensure strong passwords.

3.8 **DATA SECURITY**

a) CoreView agrees to preserve the confidentiality, integrity, and accessibility of Personal Data with administrative, technical and physical measures that conform to Industry Standards as applied to CoreView's own systems and processing environment. Unless otherwise agreed to in writing by Client, CoreView agrees that any and all Personal Data is stored, processed, and maintained solely on designated systems located in the European Union.

b) CoreView logically segregates Personal Data from CoreView's own data as well as from the data of CoreView's other customers or third parties.

3.9 **CRYPTOGRAPHY**

a) Personal Data is encrypted with a Federal Information Processing Standard (FIPS) compliant encryption product, also referred to as 140-2 compliant. Symmetric keys are encrypted with a minimum of 128-bit key and asymmetric encryption requires a minimum of 1024 bit key length. Encryption is utilized in the following instances:

   i. Personal Data that is stored on any portable computing device or any portable storage medium.

   ii. Personal Data that is transmitted or exchanged over a public network.

b) Encryption may also be required for confidential information depending upon the data classification of the confidential information.

3.10 **PHYSICAL AND ENVIRONMENTAL SECURITY**

a) Security perimeters are defined and used to protect areas that contain either sensitive, critical information or information processing facilities.

b) Secure areas are protected by appropriate entry controls designed to ensure that only authorized personnel are allowed access.

c) Physical security for offices, rooms, and facilities has been designed and applied.

d) Physical protection against natural disasters, malicious attack, or accidents has been designed and applied.

e) Equipment is protected from power failures and other disruptions caused by failures in supporting utilities.

f) All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

g) A clear desk policy for papers and a clear screen policy for facilities Processing Personal Data has been implemented and is enforced.

3.11 **OPERATIONS SECURITY**

a) Changes to the organization, business processes, information processing facilities and systems that affect information security are formally controlled.

b) Development and testing environments are separated from operational or production environments to reduce the risks of unauthorized access or changes to the operational or production environment.

c) CoreView's software development processes and environment is protected against malicious code being introduced into its product(s) future releases and/or updates.

d) Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

e) Logging facilities and log information are protected against tampering and unauthorized access. CoreView maintains access logs relevant to Personal Data for a minimum of six (6) months.

f) Rules governing the installation of software by users shall be established and implemented on operational systems.

g) **Data Backup**. Backups of Personal Data shall reside solely in the European Union. For the orderly and timely recovery of Personal Data in the event of a service interruption:

   I. CoreView stores backups of Personal Data at a secure facility.

II. CoreView encrypts all Personal Data backup data.

3.12 **NETWORK SECURITY**

a) CoreView has implemented and maintains network security controls that conform to Industry Standards including but not limited to the following:

i. CoreView utilizes firewalls to manage and restrict inbound, outbound and internal network traffic to only the necessary hosts and network resources.

ii. CoreView appropriately segments its network to only allow authorized hosts and users to traverse areas of the network and access resources that are required for their job responsibilities.

iii. CoreView ensures that publicly accessible servers are placed on a separate, isolated network segment typically referred to as the 'demilitarized zone' (DMZ).

iv. CoreView ensures that its wireless network(s) only utilize strong encryption, such as WPA2.

v. CoreView has an Intrusion Detection/Intrusion Prevention System (IDS/IPS) in place to detect inappropriate, incorrect, or anomalous activity and determine whether CoreView's computer network and/or server(s) have experienced an unauthorized intrusion.

vi. As appropriate, groups of information services, users and information systems is segregated on networks.

3.13 **COMMUNICATIONS SECURITY**

a) Formal data transfer policies, procedures and controls are in place to protect the transfer of sensitive Personal Data within electronic messaging.

b) CoreView executes a data protection and information security agreement with subcontractors/third party clients to ensure that security controls that meet CoreView requirements have been implemented.

3.14 **SYSTEM ACQUISITION, DEVELOPMENT, AND MAINTENANCE**

a) Applicable information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.

b) Personal Data involved in application services passing over public networks shall be protected from fraudulent activity, unauthorized disclosure, and modification.

c) CoreView has policies that govern the development of software and systems and how information security and integrity are established and applied during development.

d) Principles for engineering secure systems are established, documented, maintained, and applied to any information system implementation efforts.

e) CoreView shall supervise and monitor the activity of any outsourced system development.

3.15 **COREVIEW RELATIONSHIPS**

a) CoreView conducts thorough background checks and due diligence on any third and fourth parties which impact CoreView's ability to meet the requirements of the Agreement and this Addendum.

b) Client acknowledges and agrees that CoreView may, subject to the provisions of this clause 3.15 engage third-party sub-Processors in connection with the provision of the Services. CoreView has entered into an agreement with each sub-Processor containing data protection obligations not less protective than those in this Addendum with respect to the protection of Client Personal Data to the extent applicable to the nature of the Services provided by such Sub-processor.

i. CoreView's list of sub-Processors authorised at the date of execution of this Addendum is contained in Annex to the EU SCCs and is incorporated irrespective of the applicability of the Standard Contractual Clauses. The list of Sub-processors includes the identities of the Sub-processors and their country of location ("**Sub-processor Lists**"). Future updates to the list shall be made available to the Client via the notification mechanism available on CoreView's website at https://www.coreview.com/sub-processors. Each sub-processors agreement with CoreView shall include substantially similar data protection obligations as set forth in this DPA. CoreView shall provide notification of each new Sub-processor(s) before authorizing any new sub-Processor(s) to process Personal Data in connection with the provision of the Services.

ii. Client may object to CoreView's use of a new sub-Processor by notifying CoreView promptly in writing within thirty (30) days after publication of CoreView's notice in accordance with the mechanism set out in subsection (i). If Client objects to a new sub-Processor, as permitted in the preceding sentence, CoreView will use reasonable efforts to make available to Client a change in the Services or recommend a commercially reasonable change to Client's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening the Client.

iii. CoreView shall be liable for the acts and omissions of its sub-Processors to the same extent CoreView would be liable if performing the services of each Sub-processor directly under the terms of this Addendum, except as otherwise set forth in the Agreement.

3.16 **BUSINESS CONTINUITY PLANNING (BCP) AND DISASTER RECOVERY (DR)**

a) CoreView maintains an appropriate business continuity and disaster recovery plan to enable CoreView to adequately respond to and recover from business interruptions involving services provided by CoreView to Client.

I. At a minimum, CoreView tests the BCP & DR plan annually, in accordance with Industry Standards, to ensure that the business interruption and disaster objectives set forth in this Addendum have been met and will promptly remedy any failures. Upon Client's request, CoreView will provide Client with a written summary of the annual test results.

II. In the event of a business interruption that activates the BCP & DR plan affecting the Services or any Client Personal Data, CoreView will notify Client as soon as possible.

III. CoreView will allow Client or its authorized third party, upon a minimum of thirty (30) days' prior notice to CoreView's designated Security Contact, to perform an assessment of CoreView's BCP and DR plans once annually. Following notice provided by Client, the parties will meet to determine the scope and timing of the assessment.

3.17 **APPLICATION AND SOFTWARE SECURITY**

If CoreView provides hosted services to Client, CoreView agrees that its product(s) will remain secure from Software Vulnerabilities and, at a minimum, incorporate the following:

a) CoreView retains a reputable 3rd party to conduct static/manual application vulnerability scans on the application(s) software used to provide the Services to Client for each major code release and at the time of the scanning contract renewal. Results of the application testing if requested by Client, will be provided to Client in a summary report and vulnerabilities categorized as Very High, High or that have been identified as part of the OWASP top 10 and SANS top 25 within ten (10) weeks of identification will be addressed.

b) CoreView agrees at all times to provide, maintain, and support its software and subsequent updates, upgrades, and bug fixes such that the software is, and remains secure, from Common Software Vulnerabilities.

c) CoreView agrees to promptly implement updates and patches to remediate Security Vulnerabilities that are exploitable. Upon Client's request, CoreView will provide information on remediation efforts of known Security Vulnerabilities.

d) CoreView will conduct static, dynamic, automated, and/or manual security testing on its software products and/or services, hardware, devices, and systems to identify Security Vulnerabilities on an ongoing basis. Should any critical or high vulnerabilities be discovered that are likely to adversely affect Client, CoreView agrees to notify Client and create a mutually agreed upon remediation plan to resolve all such vulnerabilities identified.

e) In the event of existence of a Security Vulnerability that results in an inquiry from a regulatory agency or law enforcement agency, CoreView will cooperate and assist Client in providing a response to said party, including making appropriate CoreView personnel available to participate in face to face or telephonic meetings as reasonably requested by Client.

3.18 **DATA USE**

a) CoreView agrees that any and all Personal Data shall be used and disclosed solely and exclusively for the purposes set forth in the Agreement.

b) Personal Data shall not be distributed, repurposed or shared across other application, environments, or business units of CoreView.

3.19 **RIGHT TO AUDIT**

a) Upon a minimum of thirty (30) days' written notice to CoreView, CoreView agrees to allow a mutually agreed upon independent third party under a Non-Disclosure Agreement with CoreView to perform an audit of CoreView's policies, procedures, software, system(s), and data processing environment to confirm compliance with this Addendum on Client's behalf. Unless critical issues are identified during the audit, such audits will be restricted to one audit per any twelve (12) month period. The costs of the Client's time and any independent auditor selected by the Client shall be borne by the Client.

b) Prior to commencement of the audit, the parties will discuss the scope of the audit and the schedule. CoreView will provide reasonable support to the audit team.

c) If critical or significant issues are identified during any such audit, CoreView will provide Client a remediation plan to remedy such issues.

4. Security Incident / Data Breach

4.1 **Security Contact**. Each party shall designate a contact to serve as such party's designated Security Contact for security issues under this Agreement. In addition, the CoreView security contact is:

CoreView Security Contact:

CoreView Information Security

SUPPORT@CoreView.com

4.2 **Requirements**. CoreView takes commercially reasonable actions to ensure that Client is protected against any reasonably anticipated Security Incidents, including: (i) continual monitoring of CoreView's systems to detect evidence of a Security Incident; and (ii) maintenance of a Security Incident response process to manage and to take corrective action for any suspected or realized Security Incident. Upon

request, CoreView will provide Client with a summary of its Security Incident policies and procedures. If a Security Incident affecting CoreView products or the Services occurs, CoreView, in accordance with applicable Data Protection Laws, will take action to prevent the continuation of the Security Incident.

4.3 **Notification**. Upon determining that a Security Incident has occurred, CoreView shall notify Client without delay, and in no case later than seventy-two (72) hours, after such determination.

4.4 **Investigation and Remediation**. Upon CoreView's notification to Client of a Security Incident pursuant to Section 4.3 above, the parties shall coordinate to investigate the Security Incident. CoreView will be responsible for leading the investigation of the Security Incident but will cooperate with Client to the extent Client requires involvement in the investigation. CoreView may involve law enforcement in its discretion. Depending upon the type and scope of the Security Incident, CoreView security personnel may participate in: (i) interviews with Client's employees and subcontractors involved in the incident; and (ii) review of all relevant records, logs, files, reporting data, systems, Client devices, and other materials as otherwise required by CoreView.

4.5 In the event of a Security Incident that results in an inquiry from a regulatory agency or law enforcement agency, Client shall cooperate and assist CoreView in providing a response to such inquiry, including making appropriate Client personnel available to participate in face to face or telephonic meetings as reasonably requested by CoreView. CoreView will cooperate with Client in any litigation or investigation deemed reasonably necessary by Client to protect its rights relating to the use, disclosure, protection and maintenance of Personal Data. CoreView shall reimburse Client for reasonable costs incurred by Client in responding to, and mitigating damages caused by Security Incident that are CoreView's responsibility. CoreView will use reasonable efforts to prevent a recurrence of any such Security Incident.

4.6 **Reporting**. If requested by Client, CoreView will provide a final written incident report after resolution of a Security Incident or upon determination that the Security Incident cannot be sufficiently resolved.

5. INTERNATIONAL TRANSFERS

International transfers to CoreView and Client shall be bound by the Standard Contractual Clauses to ensure compliance with the GDPR when transferring Personal Data to CoreView in Third Countries. Client shall fulfil the role of exporter and CoreView shall comply with the importer's obligations in the Standard Contractual Clauses with respect to that transferred Personal Data. The Standard Contractual Clauses are deemed to be incorporated into and form part of this Addendum, in the form attached hereto as Appendix A. The parties undertake to meet and agree to any update and amendment to the Standard Contractual Clauses which may be required as new templates are validated and published by a Regulator.

6. RETURN OR DELETION OF PERSONAL DATA

Upon any termination or expiration of this the Services and or this Addendum, except for as provided below:

a) CoreView shall, in respect of any Personal Data transferred to it, immediately cease to use the Personal Data and shall, at the Client's option, return the Personal Data to the Client in a machine-readable format or destroy the Personal Data and all copies and extracts of the Personal Data and providing evidence to Client of such destruction having been carried out; and/or

b) Cooperate with Client to transition the Personal Data to a new Processor.

In the event CoreView is required to retain a copy of the Personal Data for compliance with legal obligations to which it is subject, it shall notify the Client of those requirements and the anticipated period for retention.

The termination of this Addendum or the Agreement for whatever cause shall not prejudice or affect the rights of any Party in respect of any breach of this Addendum or any provision herein which is expressly or by implication to survive such termination.

7. CHANGES

In the event of any change in CoreView's or Client's data protection or privacy obligations due to legislative or regulatory actions, industry standards, technology advances, or contractual obligations, CoreView and Client will work in good faith with each other to promptly amend this Addendum accordingly.

8. COUNTRY-SPECIFIC TERMS

8.1 European Economic Area Supplement ("EEA Supplement")

a) This EEA Supplement provides supplemental terms governing Processing of Personal Data for Clients established in the EEA, or where Personal Data pertains to natural persons residing in the EEA.

b) CoreView shall generally act as a Processor and Client shall generally act as a Controller. Where Client acts as a Processor, CoreView shall act as a sub-Processor to Client.

c) In the event of conflict between the terms of this EEA Supplement, the EU SCC, and the Agreement, the following order of precedence shall apply: (1) EU SCC, (2) EEA Supplement, and (3) the Agreement.

d) CoreView shall Process Personal Data only pursuant to the Agreement, as amended, unless otherwise prohibited by applicable Data Protection Laws. CoreView shall notify Client if it receives instructions from Client which in its good faith opinion violate the Data Protection Laws or the Agreement.

e) CoreView shall ensure that all personnel engaged in Personal Data Processing are informed of its confidential nature, have received appropriate training on such Processing, and are subject to confidentiality obligations regarding such data.

f) CoreView shall assist Client by appropriate technical and organization measures, to the extent reasonably possible, in responding to Data Subject requests.

g) CoreView shall provide Client with reasonable cooperation and assistance needed to fulfill Client's obligation under EU/UK Data Protection Laws to carry out a data protection impact assessment assessment related to Personal Data Processing pursuant to the Agreement and this Amendment including consultation with a Supervisory Authority regarding such assessment.

h) Upon termination or expiration of the Agreement, CoreView shall return or destroy/delete all Personal Data in Accordance with the Agreement and this Addendum. CoreView shall provide Client with information reasonably necessary to confirm its compliance with the obligations under the Agreement and this Addendum.

i) Transfers of Personal Data outside of the EEA shall be in accordance with Client's written instructions as reflected in the Agreement and this Addendum. To the extent applicable and required, such transfers shall be governed by the EU SCC, attached as Appendix A below unless the parties agree on another approved transfer adequacy mechanism.

j) Transfers and Processing of Personal Data to sub-Processors shall occur only to the extend strictly necessary for the provision of the Services under the Agreement and in accordance with applicable EU/UK Data Protection Laws. CoreView's use of sub-Processors shall be in accordance with Section 3.15(b) *supra* of this Addendum.

k) Audits of CoreView's and its sub-Processors' Processing of Personal Data shall be conducted in accordance with Section 3.19 *supra* of this Addendum.

8.2 UK Supplement

8.2.1 This UK Supplement provides supplemental terms governing Processing of Personal Data for Clients established in the UK, or where Personal Data pertains to natural persons residing in the UK.

8.2.2 CoreView shall generally act as a Processor and Client shall generally act as a Controller. Where Client acts as a Processor, CoreView shall act as a sub-Processor to Client.

8.2.3 In the event of conflict between the terms of this UK Supplement, the UK SCC, and the Agreement, the following order of precedence shall apply: (1) UK SCC, (2) EEA Supplement, and (3) the Agreement.

8.2.4 CoreView shall Process Personal Data only pursuant to the Agreement, as amended, unless otherwise prohibited by applicable Data Protection Laws. CoreView shall notify Client if it receives instructions from Client which in its good faith opinion violate the Data Protection Laws or the Agreement.

8.2.5 CoreView shall ensure that all personnel engaged in Personal Data Processing are informed of its confidential nature, have received appropriate training on such Processing, and are subject to confidentiality obligations regarding such data.

8.2.6 CoreView shall assist Client by appropriate technical and organization measures, to the extent reasonably possible, in responding to Data Subject requests.

8.2.7 CoreView shall provide Client with reasonable cooperation and assistance needed to fulfill Client's obligation under EU/UK Data Protection Laws to carry out a data protection impact assessment assessment related to Personal Data Processing pursuant to the Agreement and this Amendment including consultation with a Supervisory Authority regarding such assessment.

8.2.8 Upon termination or expiration of the Agreement, CoreView shall return or destroy/delete all Personal Data in Accordance with the Agreement and this Addendum. CoreView shall provide Client with information reasonably necessary to confirm its compliance with the obligations under the Agreement and this Addendum.

8.2.9 Transfers of Personal Data outside of the UK shall be in accordance with Client's written instructions as reflected in the Agreement and this Addendum. To the extent applicable and required, such transfers shall be governed by the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses ("UK IDTA") attached as Appendix B below unless the parties agree on another approved transfer adequacy mechanism.

8.2.10 Transfers and Processing of Personal Data to sub-Processors shall occur only to the extent strictly necessary for the provision of the Services under the Agreement and in accordance with applicable EU/UK Data Protection Laws. CoreView's use of sub-Processors shall be in accordance with Section 3.15(b) *supra* of this Addendum.

8.2.11 Audits of CoreView's and its sub-Processors' Processing of Personal Data shall be conducted in accordance with Section 3.19 *supra* of this Addendum.

Appendix A

EU STANDARD CONTRACTUAL CLAUSES

This Appendix A applies in the event Personal Data is transferred to one or more Third Countries. The Parties hereby adopt and shall adhere to the EU Standard Contractual Clauses outlined in the Annex to the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal dated to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council available at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj, as amended ("EU SCC"). The EU SCC as amended from time to time is hereby incorporated by reference.

Where applicable, Module 2 shall apply in the typical case where Coreview acts as a Processor and Client acts as Controller; Module 3 shall apply in instances where CoreView acts as a Subprocessor and Client acts as a Processor. Modules 1 and 4 shall not apply. The parties hereby elect as follows the optional clauses to the SCC:

Section I:

- Clause 7 shall apply.

Section II

- Clause 9(a): Option 2 shall apply, with CoreView to notify Client at least 30 days in advance of changes to the Sub-processor Lists referenced in Section 3.15(b)(i) hereto.
- Clause 11(a): optional language shall not apply.
- Clause 13: If applicable, the competent Supervisory Authority shall be the Supervisory Authority of the Republic of Ireland.

Section IV

- Clause 17: Option 1 shall apply whereby the SCC shall be governed by the laws of the Republic of Ireland.
- Clause 18(b): Republic of Ireland

APPENDIX TO THE STANDARD CONTRACTUAL CLAUSES

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s).

ANNEX I

A. LIST OF PARTIES

Data exporter [TO BE COMPLETED FOR EACH CUSTOMER]

Name: _____

Address: _____

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

_____

Activities relevant to the data transferred under these Clauses:

Utilization of the Services as set out in the Agreement

Signature and date: _____

Role (controller/processor): Controller

Data importer

Name: CoreView S.r.l.

Address: Via Agostino Bertani 6, 20154 Milano, Italy

Contact person's name, position and contact details:

FAO CoreView DPO, The DPO Centre Limited, 50 Liverpool Street, London EC2M 7PY, UK, privacy@coreview.com

Activities relevant to the data transferred under these Clauses:

CoreView S.r.l. is a provider of subscription software services which processes personal data upon the instruction of the data exporter in accordance with the terms of the Agreement executed by both parties.

Signature and date: _____

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Directors, officers, employees, contractors, contacts, and business associates, of the Client or their Affiliates.

Categories of personal data transferred

Name, first name, last name

Address information (e.g., street, number, postal code, city, PO box)

Contact information (e.g., phone number, fax number, cell phone number, email address)

Identification number (e.g., ID, client number, employee number)

Position, department, organizational assignment

Communications data (e.g., phone number, fax number, cell phone number, email address) and communication content

Log and protocol information

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose

limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

None.

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

Continuous

Nature of the processing

Operations necessary to deliver Services as agreed between Parties including organisation, structuring, adaptation or alteration, retrieval, use, disclosure by transmission, dissemination or making available, alignment restriction, erasure, or destruction of personal data.

Purpose(s) of the data transfer and further processing

CoreView will be collecting activity data from Client's Microsoft 365 tenant and Azure AD sign-in activity. IT services/consultation services/services in connection with processing of personal data

Provision of software/solutions

Operation of the software/solutions

Programming services

Maintenance and support

Consultation services

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

Duration of the subscription and as set out in the Addendum.

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

Hosting and operating the Platform for the duration of the subscription.

C. COMPETENT SUPERVISORY AUTHORITY

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

The Supervisory Authority of the Republic of Ireland.

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

See Section 3 of the Addendum, *supra*.

ANNEX III – LIST OF SUB-PROCESSORS

The controller has authorised the use of the sub-processors listed at http://www.coreview.com/sub-processors.

Switzerland Addendum

1. For the purpose of interpreting this Addendum, the following terms shall have the meanings set out below:

a) "**Data Protection Laws**" (as used in the DPA) includes Swiss Data Protection Laws.

b) "**Controller"** includes "**Controller of the Data File**" as defined under the FADP (as defined below).

c) "**Data Subject**" includes the natural persons whose Personal Data are Processed.

d) "**EU SCCs**" means as defined in the DPA.

e) "**Personal Data**" includes "**Personal Data**" as defined under the FADP.

f) "**Processing**" includes "**Processing**" as defined under the FADP.

g) "**Swiss Data Protection Laws**" includes the Swiss Federal Act on Data Protection of 19 June 1992 ("**FADP**") and the Ordinance to the Federal Act on Data Protection ("**OFADP**"), as they may be amended from time to time.

h) "**Restricted Transfer of Swiss Data**" includes any transfer of Personal Data (including data storage in foreign servers) subject to the FADP to a Third Country or an international organization.

i) "**Third Country**" means a country outside the Swiss Confederation.

2. With regard to any Restricted Transfers of Swiss Data within the scope of the DPA, one of the following transfer mechanisms shall apply, in the following order of precedence:

(a) The inclusion of the Third Country, a territory, or one or more specified sectors within that Third Country, or the international organization in question to which Personal Data is to be transferred in the list published by the Swiss Federal Data Protection and Information Commissioner of states that provide an adequate level of protection for Personal Data within the meaning of Swiss Data Protection laws.

(b) The EU 2021 Standard Contractual Clauses (insofar as their use constitutes an "appropriate safeguard" under Swiss Data Protection Laws).

(c) Any other lawful transfer mechanism, as laid down in Swiss Data Protection Laws.

3. EU SCCs:

(a) This "**Switzerland Addendum**" hereby incorporates the above completed EU 2021 Standard Contractual Clauses.

(b) The content of EU SCCs Annex I and Annex II is set out above.

(c) The text contained in this Switzerland Addendum supplements and updates the EU SCCs.

(d) The Parties agree to apply the modules selected in Annex 2 of the Agreement of which the DPA forms a part.

(e). With respect to Clause 17 of the EU SCCs, the Parties shall read the selected law as that of the Swiss Confederation.

(f). With respect to Clause 18 of the Standard Contractual Clauses, the Parties shall read the chosen courts as the Swiss courts as an alternative place of jurisdiction for data subjects habitually resident in Switzerland.

(g) The term "**member state**" included in the EU SCCs must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18 (c) of the EU SCCs.

4. With respect to Restricted Transfers of Swiss Personal Data, the Parties acknowledge that the EU SCCs also protect the data of legal entities until the entry into force of the revised FADP.

Appendix B

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses ("UK IDTA")

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	Per the EU SCCs and the Agreement	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: Per the EU SCCs to which this IDTA is appended and the Agreement Trading name (if different): N/A Main address (if a company registered address): Per the EU SCCs to which this IDTA is appended Official registration number (if any) (company number or similar identifier):	Full legal name: Per the EU SCCs to which this IDTA is appended and the Agreement Trading name (if different): N/A Main address (if a company registered address): Per the EU SCCs to which this IDTA is appended Official registration number (if any) (company number or similar identifier):
Key Contact	Full Name (optional): Per the EU SCCs to which this IDTA is appended Job Title: Per the EU SCCs to which this IDTA is appended Contact details including email: Per the EU SCCs to which this IDTA is appended	Full Name (optional): Per the EU SCCs to which this IDTA is appended Job Title: Per the EU SCCs to which this IDTA is appended Contact details including email: Per the EU SCCs to which this IDTA is appended
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: Per the EU SCCs to which this IDTA is appended

	Reference (if any): N/A Other identifier (if any): N/A Or ☒ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1	No	N/A	N/A	N/A	N/A	N/A
2	Yes	Yes	No	general authorization	30 days	No
3	Yes	Yes	No	general authorization	30 days	No
4	No	N/A	N/A	N/A	N/A	N/A

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: Per the EU SCCs to which this IDTA is appended
Annex 1B: Description of Transfer: Per the EU SCCs to which this IDTA is appended
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: Per the EU SCCs to which this IDTA is appended
Annex III: List of Sub processors (Modules 2 and 3 only): Per the EU SCCs to which this IDTA is appended

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 0: ☐ 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 0.
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 0 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 0 to 0 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 0, the provisions of Section 0 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 0 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 0) 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 0, 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.