CoreView

DATA PROTECTION AND INFORMATION SECURITY ADDENDUM

Approved for Use - September 2021

This agreement consists of 25 pages including this one. It contains technical and organizational measures for data security and the European Commission's Standard Contractual Clauses (SCCs) between the data controller as exporter and the data processor as importer to to comply with the terms of art. 46, par. 2, lett. c) and lett. d) of GDPR.

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 purchase of services (identified either as "Services" or otherwise in the applicable agreement, and hereinafter defined as "Services") from CoreView S.r.l. ("CoreView") to reflect the parties' agreement with regard to 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. Throughout the term of the Agreement and for as long as CoreView controls, possesses, stores, transmits, or processes Personal Information as part of the Services, CoreView and Client will comply with the requirements set forth in this Addendum.

1. Definitions

"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.

"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

"Critical Infrastructure Information" (CII) means information about Client's network architecture as well as that of its customers, including information about application access, remote access procedures, user ID's and passwords, the location and capability of central offices, data centers, data warehouses, network access points, network points of presence and other critical network sites, as well as the network elements and equipment within them, and includes any information which Clients reasonably identifies as critical infrastructure information.

"Data Protection Laws" mean all applicable laws, standards, guidelines, policies, regulations and procedures applicable to CoreView pertaining to data security, confidentiality, privacy, and breach notification. Data Protection Laws includes the EU General Data Protection Regulation 2016/679, as the same may be amended from time to time ("GDPR").

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

"Personal Data" also known as Personally Identifiable Information (PII), is information of Client customers, employees and subcontractors held or accessed by CoreView that can be used on its own or combined with other information to identify, contact, or locate a 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.

"Regulator" means the data protection supervisory authority which has jurisdiction over a data controller's processing of Personal Data.

"Third Countries" means all countries outside of the scope of the Data Protection Laws of the European Union or the European Economic Area ("EEA"), excluding countries recognized by the 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.

Any terms not otherwise defined herein have the meaning assigned under applicable Data Protection Laws.

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. 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 necessary to provide the Services or otherwise to comply with applicable Data Protection Laws;

b) 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;

c) 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 (taking into account 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;

d) Client warrants that: (a) 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 (b) all notices have been given to, and 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;

e) 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 will immediately inform Client.

f) 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.

g) CoreView shall, to the extent legally permitted, 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 (“right to be forgotten”), 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. To the extent legally permitted, Client shall be responsible for any costs arising from CoreView’ provision of such assistance.

3. Information Security Expectations:

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 retain 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 (IDS/IPS) System 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 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 Agreement with respect to the protection of Client Data to the extent applicable to the nature of the Services provided by such Sub-processor.

i. CoreView's current list of Sub-processors is located on CoreView's website. The list of Sub-processors includes the identities of the Sub-processors and their country of location ("**Sub-processor Lists**"). CoreView shall provide notification on the Sub-processor page 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 ten (10) business 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. If CoreView is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Client's sole remedy is to terminate the applicable Order with respect only to those Services which cannot be provided by CoreView without the use of the objected-to new Sub-processor by providing written notice to CoreView.

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 Client or 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 at Client's expense to confirm compliance with this Addendum. Unless critical issues are identified during the audit, such audits will be restricted to one audit per any twelve (12) month period.

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 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) CoreView's systems are continually monitored to detect evidence of a Security Incident; (ii) CoreView has a Security Incident response process to manage and to take corrective action for any suspected or realized Security Incident; and (iii) 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. Without undue delay (but no later than forty-eight (48) hours) after CoreView's determination that a Security Incident has occurred, CoreView will notify Client of the incident.

4.4 Investigation and Remediation. Upon CoreView's notification to Client of a Security Incident, the parties will 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 said party, 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, at Client's expenses, 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 will reimburse Client for reasonable costs incurred by Client in responding to, and mitigating damages caused by Security Incident that are under CoreView 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.

In order to ensure adequate safeguards for the Personal Data where it is transferred to CoreView in a Third Country, Client shall comply with the exporter's obligations in the standard contractual clauses for the transfer of Personal Data to processors established in third countries set out in the European Commission Decision 2010/87/EC ("Standard Contractual Clauses") and CoreView shall comply with the importers obligations in the Standard Contractual Clauses in respect of 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 Exhibit 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 the Regulator.

6. CHANGES

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

[Client]	**CoreView S.r.l.**
By: ______________________	By: ______________________
Name: ______________________	Name: ______________________
Title: ______________________	Title: ______________________

EXHIBIT A

Standard Contractual Clauses (Processors)

For the purposes of EU General Data Protection Regulation 2016/679for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation:...

Address: ....

Tel.:..; **e-mail:**...............................

Other information needed to identify the organisation:

....

(the data **exporter**)

And

Name of the data importing organisation: CoreView S.r.l.

Address: Via Agostino Bertani 6, 20154, Milan, Italy

Tel.: +39.028.725.9395 **E-mail:** privacy@coreview.com

Other information needed to identify the organisation: Not applicable

……………………………………………………………………

(the data **importer**)

each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix.

STANDARD CONTRACTUAL CLAUSES

Controller to Processor

SECTION I

Clause 1
Purpose and scope

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

(b) The Parties:

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

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

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

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

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

Clause 2
Effect and invariability of the Clauses

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

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

Clause 3
Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

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

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

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

(v) Clause 13;

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

(vii) Clause 16(e);

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

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

Clause 4
Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

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

Clause 5
Hierarchy

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

Clause 6
Description of the transfer(s)

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

Clause 7
Docking clause

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

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

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8
Data protection safeguards

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

8.1 Instructions

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

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

8.2 Purpose limitation

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

8.3 Transparency

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

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

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

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the

Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

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

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

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

8.7 Sensitive data

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

8.8 Onward transfers

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

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

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

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

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

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

8.9 Documentation and compliance

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

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

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

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

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

Clause 9

Use of sub-processors

(a) The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least thirty (30) days prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.8 The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

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

Clause 10

Data subject rights

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

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

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

Clause 11
Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body[1] at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it or follow a particular sequence in seeking redress.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

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

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

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

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

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

Clause 12
Liability

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

[1] The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

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

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

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

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

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

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

Clause 13
Supervision

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

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

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

Clause 14
Local laws and practices affecting compliance with the Clauses

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

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

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

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

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

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

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

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

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

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

15.1 Notification

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

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

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

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

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

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

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

15.2 Review of legality and data minimisation

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

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

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

SECTION IV – FINAL PROVISIONS

Clause 16
Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

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

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

Clause 17
Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Italy.

Clause 18
Choice of forum and jurisdiction

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

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

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

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

On behalf of the data importer:

Name (written out in full): _____________

Position: _________________

Address: Via Agostino Bertani 6, 20154 Milan, Italy

Other information necessary in order for the contract to be binding (if any): N/A

Signature……………………………………….

(stamp of organisation)

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

Name: ____

Address: ____

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

____

Activities relevant to the data transferred under these Clauses:

____

____

Signature and date: ____

Role (controller/processor): Contoller

Data importer

Name: CoreView S.r.l.

Address: Via Agostino Bertani 6, 20154 Milano, Italy

Contact person's name, position and contact details:

Matthew H.J. Kim, General Counsel, 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.

End users

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

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

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

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.

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.

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

____

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

As described in Section 3 of the Addendum.

ANNEX III – LIST OF SUB-PROCESSORS

As available on www.coreview.com