Data Processing Agreement (DPA)

This data processing agreement ("Agreement") is entered into between

CoSoSys SRL, a Romanian company, with registered office at Somesului str., nr.14, Ground Fl., 400145, Cluj-Napoca, Romania, and its Affiliates, hereinafter named "**Processor**" or "**CoSoSys**" or "**Supplier**",

and

_____ a _____ company, with registered office at _____ _____, hereinafter named "**Controller**" or "**Client**",

hereinafter collectively referred to as 'Parties' and individually as a 'Party'.

The Parties have agreed on the following Agreement in order to meet the requirements of the Regulation 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 and repealing Directive 95/46/EC ("GDPR") and to ensure the protection of the rights of the data subjects.

1.Background

1.1 The Parties have previously entered into one or more of the following agreements:

a.) if the Controller is an end customer ("**End Customer**") of a CoSoSys on premise Products and Services, an End User License Agreement ("**EULA**");

b.) if the Controller is an End Customer of a CoSoSys Hosted Products and Services, a Service Agreement ("**SA**") and a Service Level Agreement ("**SLA**");

c.) if the Controller is an End Customer of a Master License Agreement ("**MLA**");

d.) If the Controller is a prospective Customer an Evaluation Agreement or an EULA;

hereinafter collectively referred to as "**The Main Agreement**".

1.2 This Agreement, the Main Agreement and the documents annexed to the Main Agreement and to this Agreement, shall collectively constitute the entire agreement between the Parties.

1.3 This Agreement sets forth the rights and obligations of the Parties when the Processor processes personal data on behalf of the Controller.

1.4 The Agreement has been designed to ensure the Parties' compliance with art. 28 para. (3) of GDPR.

1.5 In the context of the performance of the Main Agreement, the Processor processes personal data on behalf of the Controller, in accordance with the Agreement.

1.6 The Agreement shall take priority over any similar provisions contained in other agreements between the Parties.

1.7 The Agreement shall not exempt the Parties from any obligations to which they, either independently or jointly, are subject pursuant to GDPR or other legislation.

2. Definitions

"Affiliates" means any firm, person or entity controlling, controlled by or under common control with a Party (where "control" shall mean the ownership or control, whether directly or indirectly, of more than fifty percent (50%) of the outstanding shares or voting interests of an entity).

"Personal Data" means any personal data for which the Client is the controller, under the applicable data protection laws and regulations, that the Client shares or otherwise provides access to Supplier in connection with its use of Supplier's products or services or for which Client is otherwise a data controller.

"Applicable Data Protection Laws and Regulations" means

a.) EU Regulation 2016/679 on the protection of natural persons regarding the processing of personal data and on the free movement of such data (GDPR) and

b.) any and all applicable national data protection laws.

"Sub-processor" means any entity which provides services to Supplier which include processing of Personal Data.

"Controller" means the Client. For avoidance of doubt a Client is an End Customer that uses or evaluates the Supplier's Product and/or Services.

"Processor" means the Supplier.

"Hosted products" means My Endpoint Protector, Sensitivity.io., Hosted Endpoint Protector.

"Products and Services" means Endpoint Protector as on-premise offering (Virtual Appliance, Amazon Machine Image etc.), and/or Technical Support Services.

3. The rights and obligations of the Controller

3.1 Controller shall, in its use of the Products and Services, process Personal Data in accordance with the requirements of the Applicable Data Protection Laws and Regulations. For the avoidance of doubt, Controller's instructions for the processing of Personal Data shall comply with the Applicable Data Protection Laws and Regulations. Controller shall have the sole responsibility for the accuracy, quality, and legality of Personal Data.

3.2 The Controller is responsible for ensuring that the processing of Personal Data takes place in compliance with the GDPR, the applicable EU or EEA Member State data protection provisions and the Agreement.

3.3 The Controller has the right and obligation to make decisions about the purposes and means of the processing of Personal Data.

3.4 The Controller shall be responsible, among other, for ensuring that the processing of Personal Data, which the Processor is instructed to perform, has a legal basis.

4. Instructions

4.1 The Processor shall process Personal Data only on documented instructions from the Controller, unless required to do so by EU or EEA Member State law to which the Processor is subject. Such instructions shall be specified in Exhibit 1. Subsequent instructions in connection with the Agreement can also be given by the Controller throughout the duration of the processing of Personal Data, but such instructions shall always be documented and kept in writing, including electronically.

4.2 The Processor shall immediately inform the Controller if instructions given by the Controller, in the opinion of the Processor, contravene the GDPR or the applicable EU or EEA Member State data protection provisions.

5. Confidentiality

5.1 Processor shall treat Personal Data as confidential information and shall only grant access to the Personal Data being processed on behalf of the Controller to persons under the Processor's authority or instructions who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis.

5.2 The Processor shall at the request of the Controller demonstrate that the concerned persons under the Processor's authority are subject to the abovementioned confidentiality.

6. Security of processing

6.1 The Controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:

1. pseudonymisation and encryption of Personal Data;
2. the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;
3. the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;
4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

6.2 The Processor shall implement at least the minimum security measures specified in Exhibit 2 to mitigate those risks. The Processor ensures at its own costs, proper implementation of the minimum security measures.

6.3 The Processor shall assist the Controller in ensuring compliance with the Controller's obligations pursuant to art. 32 GDPR, by *inter alia* providing the Controller with information concerning the technical and organisational measures already implemented by the Processor pursuant to art. 32

GDPR along with all other information necessary for the Controller to comply with the Controller's obligation under art. 32 GDPR.

7. Audit rights of the Controller

7.1 On the condition that Controller and Processor have entered into an applicable non-disclosure agreement, at its own cost, and upon 30 days' prior written notice, the Controller shall have the right to conduct audits, including inspections, in consultation with the Processor or to have them implemented by independent inspectors in case of a security breach. The Controller shall have the right to verify compliance of the Processor with this Agreement and the Processor shall provide the Controller all information and documentation reasonably necessary to demonstrate Processor's compliance with the obligations laid down in this Agreement.

7.2 The Processor shall be required to provide the supervisory authorities, which pursuant to Applicable Data Protection Laws and Regulations have access to the Controller's and Processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the Processor's physical facilities on presentation of appropriate identification.

7.3 The scope of the audit shall not require Processor to disclose to Controller or its independent inspectors to access:

7.3.1 Any information or data of any other client of the Processor;

7.3.2 Any internal accounting or financial information of the Processor;

7.3.3 Any information or data that the Controller or its independent inspectors may seek to access for any other reason than the good faith fulfilment of the Processor's obligations of compliance with the terms of this Agreement and the Applicable Data Protection Laws and Regulations;

7.3.4 Any information or data, that in the Processor's opinion is compromising the security of Processor's systems and premises, or causes the Processor to breach any of its obligations under the Applicable Data Protection Laws and Regulations or Processor's privacy, security, confidentiality obligations to any other client or contractor of the Processor;

7.3.5 Any trade secret of the Processor.

8. Sub-processors

8.1 The Controller gives a general authorisation to Processor to engage another processor (Sub-processor) for the fulfilment of the Agreement.

8.2 On the effective date of the Agreement the Controller authorises the engagement of the following Sub-processors: https://www.endpointprotector.com/legal/data-sub-processor-list. The Processor implements a mechanism whereby the Controller is able to receive a notification prior to any appointment of a new Sub-processor, by the Processor. New Sub-processors will be considered authorised unless Controller, upon reasonable grounds, objects to the authorisation of a new Sub-processor within fourteen (14) days following the notice of the intended appointment. In case of an objection, the Parties must work together in good faith to address the concerns.

8.3 Where the Processor engages a Sub-processor for carrying out specific processing activities on behalf of the Controller, substantially similar data protection obligations as set out in this Agreement shall be imposed on that Sub-processor by way of a contract or other legal act under EU or EEA Member State law, in particular providing sufficient guarantees regarding the implementation of appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Agreement and the Applicable Data Protection Laws and Regulations.

8.4 If the Sub-processor does not fulfil his data protection obligations, the Processor shall remain fully liable to the Controller as regards the fulfilment of the obligations of the Sub-processor towards the Controller. This does not affect the rights of the data subjects under the GDPR – in particular the right to an effective judicial remedy against a controller or processor (art. 79 GDPR) or the right to compensation (art. 82 GDPR) – against the Controller and the Processor, including the Sub-processor.

8.5 If the Sub-processor is located in a third country or in an international organization the transfer of Personal Data from Processor to Sub-processor shall always take place in compliance with chapter V GDPR.

9. International Data transfer

9.1 Certain hosted products enable the Controller to choose whether to host such product in the European Union, the United States of America or other countries outside the European Union. This selection takes place at the request of the Controller.

9.2 The Processor shall ensure that there are appropriate measures taken for international transfers of Personal Data outside of the European Union. If Personal Data originating in the European Economic Area (the "EEA"), Switzerland, and/or the United Kingdom is transferred by Processor to a Sub-processor in a country that has not been found to provide an adequate level of protection under Applicable Law by the European Commission, the Parties agree that the terms of the transfer shall be governed by the Standard Contractual Clauses published by the European Commission. Whilst the Processor had already entered into Standard Contractual Clauses with its Sub-Processors pursuant to the European Commission Decisions 2004/915 and 2010/87, following the adoption of the European Commission Decision 2021/914 on Standard Contractual Clauses for the transfer of Personal Data to third countries on 4 June 2021, Processor commits to updating the existing Standard Contractual Clauses with its existing Sub-Processors, in accordance with the new Decision, within the deadlines indicated in this Decision. The parties agree that: (i) pursuant to Clause 5(h) and Clause 11 of the Standard Contractual Clauses, Processor may engage new Sub-processors in accordance with Section 8 of this DPA; and (ii) the Sub-processor agreements referenced in Clause 5(j) and certification of deletion referenced in Clause 12(1) of the Standard Contractual Clauses shall be provided only upon Controller's written request. The respective Standard Contractual Clauses may be shared with any Data Subjects if required under Applicable Law.

9.3 In case of the use of a Hosted Product, Controller may elect to grant third parties visibility to the Controller's data or content. Controller understands that the user profile information for the Hosted Product may be visible to third parties, such as Amazon Web Services, and Controller hereby accepts and understands, that nothing in this Agreement prohibits Processor from making the Controller's data or content visible to third parties consistent with this paragraph and as directed by the Controller through the Hosted Product.

9.4 In case transfers to third countries or international organisations, which the Processor has not been instructed to perform by the Controller, are required under EU or EEA Member State law to which the Processor is subject, the Processor shall inform the Controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

9.5 Without documented instructions from the Controller, the Processor therefore cannot within the framework of the Agreement:

1. transfer Personal Data to a controller or a processor in a third country or in an international organisation;

2. transfer the processing of Personal Data to a Sub-processor in a third country.

10. Assistance to the Controller

10.1 Taking into account the nature of the processing, the Processor shall assist the Controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the Controller's obligations to respond to requests for exercising the data subject's rights.

10.2 In addition to the Processor's obligation to assist the Controller pursuant to clause 6.3, the Processor shall furthermore, taking into account the nature of the processing and the information available to the Processor, assist the Controller in ensuring compliance with:

1. the Controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority;

2. the Controller's obligation to without undue delay communicate the personal data breach to the data subject;

3. the Controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (data protection impact assessment – "**DPIA**");

4. the Controller's obligation to consult the competent supervisory authority prior to processing where a DPIA indicates that the processing would result in a high risk in the absence of measures taken by the Controller to mitigate the risk.

11. Notification of personal data breach

11.1 In case of any personal data breach, the Processor shall, without undue delay, after having become aware of it, notify the Controller of the personal data breach.

11.2 In accordance with art. 10.2 point 1., the Processor shall assist the Controller in notifying the personal data breach to the competent supervisory authority, meaning that the Processor is required to assist in obtaining the information listed below which shall be stated in the Controller's notification to the competent supervisory authority:

1. the nature of the Personal Data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of Personal Data records concerned;

2. the likely consequences of the personal data breach;

3. the measures taken or proposed to be taken by the Controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

12. Deletion and return of Personal Data

12.1 On the termination or expiration of the Main Agreement the Processor shall be under the obligation to return all the Personal Data and copies of such data to Controller or securely destroy them and, upon request, certify this to the Controller that it has taken such measures, unless local, Union or EEA Member State law requires storage of Personal Data. In such case, Processor shall preserve the confidentiality of the Personal Data retained by it and that it will only actively process such Personal Data after such date in order to comply with Applicable Data Protection Laws and Regulations.

12.2 The Processor shall retain documentation that proves that data was processed in an orderly and contractual manner after the respective contract period has elapsed in accordance with respective retention periods beyond the end of the Main Agreement.

13. Controller's and Processor's contact points

13.1 The Parties may contact each other using the following contact points:

For Controller:

Name: _____

Position: _____

Telephone: _____

E-mail: _____

For Processor:

Name: Bogdan Melinte

Position: Data Protection Officer (DPO)

Telephone: 0040-264-593-110

E-mail: privacy@cososys.com

13.2 The Parties shall be under an obligation to continuously to inform each other of changes to contact points.

14. Term and Termination

14.1 The Agreement shall become effective on the date of both Parties' signature. If the Controller makes any deletions or other revisions to the Agreement without obtaining the Processor's prior written approval, then the Agreement will be null and void. The signed and completed Agreement must be submitted to Processor via email at privacy@cososys.com.

14.2 The person signing the Agreement warrants and represents to Processor that he or she has the legal authority to bind Controller and is lawfully authorised to enter into contracts.

14.3 Both Parties shall be entitled to require the Agreement renegotiated in good faith if changes to the law or to the Main Agreement should give rise to such renegotiation.

14.4 A fee for this Agreement is not required.

14.5 The Processor's liability to the Controller in connection with any issue arising out of, or in connection with this Agreement, shall not, in any case, exceed the Processor's limitations on liability set out in the Main Agreement. The limitations on liability set out in the Main Agreement shall apply in aggregate across both the Main Agreement and this Agreement.

14.6 The governing law and jurisdiction of this Agreement shall be the same as set out in the Main Agreement.

14.7 This Agreement is dependent on the existing Main Agreement as described in paragraph 1.1 of this Agreement. The cancellation or termination of the Main Agreement shall automatically trigger the termination or expiration of this Agreement. The Parties' rights under the Applicable Data Protection Laws and Regulations shall survive the termination of this Agreement and the Main Agreement, for the duration mandated by the applicable law.

14.8 The Agreement shall apply for the duration of the Main Agreement and it cannot be terminated during this period, unless another agreement governing the provision of personal data processing services has been agreed between the Parties.

14.9 Any modifications to this Agreement shall be in written form signed by both Parties.

On behalf of the Controller	**On behalf of the Processor**
Name	Name
Position	Position CEO
Date	Date
Signature	Signature

Exhibit 1
Data processing

This Exhibit describes the processing the Processor performs on behalf of the Controller.

1. **Purpose of data processing**

The Controller's Personal Data are subject to the following processing activities:

a.) Providing products and services purchased by the Controller under the Main Agreement;
b.) Providing technical support services;
c.) Hosting the hosted products;
d.) Processing in accordance with the Main Agreement and applicable Order Form(s);
e.) Processing initiated by the Controller in its use of the Services;
f.) Providing the product for evaluation (trial) purposes;
g.) Processing to comply with other documented reasonable instructions provided by Controller (e.g., remote support sessions, via email, chat, phone or online calls, etc.) where such instructions are consistent with the terms of the Agreement.

The Processor provides products and services designed for data loss prevention, a solution that is created to detect and prevent security threats within systems, devices, files and other data made available by the Controller. The content of any information held in these systems, devices, files and other data is not determined by the Processor, but it is solely determined by the Controller, and the Processor processes these data made available by the Controller for the sole purpose of providing the data loss prevention products and services and support services procured by the Controller.

2. **Types of Personal Data**

For the purposes mentioned above, the Processor processes on behalf of the Controller the following Personal Data:

a.) Names
b.) Business Email addresses
c.) IP addresses
d.) Business Telephone numbers

3. **Categories of data subjects**

The Processor processes on behalf of the Controller the Personal Data of Controller's employees and contractors who are in contact with Processor in connection with the Main Agreement.

4. **Duration of processing**

The Processor processes the above-mentioned Personal Data on behalf of the Controller for the duration of the Main Agreement and after its termination as it is necessary to be compliant with local and international legislation.

Exhibit 2
Security Measures of Processor

1. **Physical Access Control**
   - Physical access control system
   - Each employee/visitor has a unique access badge (user ID)
   - User IDs are not shared or used by anyone other than the user to whom it was assigned
   - User IDs are disabled immediately on the day of termination of the employee's contract
   - Access logs
   - Alarms on all doors
   - Badge readers on all entrances
   - Video surveillance on company premises
   - 24/7 security guard

2. **Physical security control**
   - Reasonable physical protection against damage from fire, flood, earthquake, and other forms of natural or man-made disaster for facilities, such as: climate control system, temperature and humidity sensor, raised floor, smoke detector, heat detector, fire suppression system, alarm notification system, on premise certified fireman
   - Uninterruptible power supply (UPS)
   - Generator with the capacity to supply power for more than 24 hours with onsite fuel capacity

3. **Data Access Control**
   - Information classification policy in place
   - Access rights are granted to authorized personnel based on the information classification policy
   - Employees have a unique user IDs and passwords for their own use
   - Employees are required to have a length of minimum 8 characters and must not be equal to, or derivative of the user ID and must contain at least one alphabetic and one non-alphabetic character
   - All physical confidential documentation, including accounting documentation is closed in restricted areas with access by key
   - Portable devices are encrypted using CoSoSys products
   - All servers carrying confidential and Personal Data are encrypted
   - All computers and laptops are required to use an anti-virus solution

4. **Input control for hosted products**
   - All communication between the client software and the backend system is performed over HTTPS to secure data in transit, establishing trusted communication via certificates and server validation

5. **Organizational control**
   - New employees are required to undertake a data protection and security training as part of their onboarding process
   - A dedicated IT security team is appointed to manage internal risk and incident response process
   - Two data protection officers are appointed and can be reached at privacy@cososys.com

6. **Operational control**
   - background verification checks are carried out on all supplier candidate for employment
   - security roles and responsibilities of employees are defined and documented