ERMES CYBER SECURITY
END-USER LICENSE AGREEMENT

END-USER LICENSE AGREEMENT

1. Introduction

1.1. The following are the terms and conditions that govern the End-User License Agreement (referred to as "**EULA**" in the following text) for the Software.

1.2. The Annexes and Appendices, together with the EULA, form an integral and substantial part of the EULA.

2. Definitions

2.1. For the purposes of this EULA, words with initial capital letters are defined in the Glossary as provided in Annex A, in which terms defined in the plural are also considered defined in the singular, and vice versa.

3. Acceptance of the EULA

3.1. By using the Software, the User agrees to use it in accordance with all the terms and conditions specified in the EULA.

3.2. The EULA constitutes a legally binding contract between ECS and the Customer, under which the Parties commit to fulfilling the obligations specified in the EULA.

3.3. If the acceptance is made on behalf of one's employer or another legal entity (the Customer), the User represents and warrants that (i) they have full legal authority to bind their employer or the legal entity that is the recipient of this EULA; (ii) they have read and understood this EULA, and (iii) they accept this EULA on behalf of the represented party.

4. Subject

4.1. By accepting the EULA (directly or through the User as per the previous article), the Customer has the right to use a valid, non-exclusive, non-transferable, and non-free worldwide license, for the duration corresponding to the EULA's term, for the installation and use of the Software on the devices and in the manner specified in the sales contract through which the Customer acquired the Software from the Reseller, in accordance with all the terms and conditions specified in the EULA (the "License"). The costs of this License are borne by the Customer.

5. Use of the Software: Customer's Obligations

5.1. Given that the use of the Software is directly connected to the operation and use of the Services and Resources, the User agrees to use the Software in a manner that:

a) Do not disrupt, damage, or impair one or more SaaS Services, servers, or the network connected to the Resources, or violate security measures, procedures, policies, or rules of the network connected to the SaaS Services, including the rules of conduct applicable to users of services accessible via the internet (Netiquette);

b) Do not intentionally or unintentionally violate applicable laws in Italy, in the country where the User is located, or any other laws applicable to the User's activities;

c) Do not engage or occupy the Resources or prevent access to one or more SaaS Services, Resources, and their use without the permission of ECS;

d) Do not send unsolicited or unwanted email;

e) Do not impersonate ECS or others;

f) Do not forge headers or otherwise manipulate identifiers (including URIs) in an attempt to disguise the origin of any Content transmitted using one or more SaaS Services;

g) Do not use in any way one or more SaaS Services, servers, or the network connected to the Resources to engage in or allow Third Parties to engage in scraping or other data acquisition activities by bypassing the normal functionality of the Connection Interfaces.

5.2. The User must provide devices and connectivity services suitable for enabling the efficient functioning of the Connection Interfaces, following the technical specifications provided by ECS, which may be updated over time.

6. Use of SaaS Services and Resources: Notices and Disclaimer

6.1. ECS monitors the operation of Resources and SaaS Services from the European Union and will use its reasonable capabilities and attention to try to maintain the availability and functionality of Resources and SaaS Services even outside the aforementioned geographic area. However, it does not guarantee that Resources and SaaS Services will be available at all times.

6.2. In particular, any liability is expressly excluded for cases in which the malfunction of Resources and SaaS Services depends on:

a) Unauthorized or incorrect use of the Software, Resources, and SaaS Services;

b) The failure or partial operation of the Customer's or User's devices or equipment, or non-compliance with the technical specifications provided by ECS;

c) Events dependent on the responsibility of internet access providers or telephone line operators;

d) Malfunctions of the internet or telephone network;

e) Unauthorized access to the Resources and SaaS Services by the User or by a third party, or alterations in the transmission of Content;

f) Force majeure or causes beyond the control or fault of ECS.

6.3. The Resources contain links to other resources to which Users may be redirected. These resources are not monitored or controlled by ECS, and therefore, ECS is not responsible for them.

6.4. ECS makes its best efforts to ensure that the Resources and SaaS Services are easily usable with as many Connection Interfaces as possible. However, ECS expressly excludes any guarantee that the Resources and SaaS Services will work with every possible Connection Interface. The Customer is aware of and accepts this limitation of functionality of the Resources and SaaS Services.

7. Copyright

7.1. Except as otherwise provided, the Resources, SaaS Services, Contents, Connection Interfaces, and Software are the exclusive property of ECS and are protected by Italian and international laws, particularly those related to copyright.

7.2. Acceptance of the EULA imposes an obligation on the User not to perform, and not to authorize others to perform, the following operations on the Software or any part thereof (by way of example and not limited to: the graphical interface), including any updates, improvements, and/or modifications: copying (to any medium or logical resource), decompilation, disassembly, reassembly, attempts to derive the source code, decoding, modification, creation of derivative software, leasing, renting, lending, selling, redistributing, sublicensing. These obligations also apply to the use of all Services and Resources used by the User based on the Software.

7.3. The User expressly agrees not to perform (and not to authorize others to perform) the aforementioned operations, including the technical documentation provided and registered trademarks and names.

7.4. Performing one or more of the aforementioned operations constitutes a contractual breach and results in the automatic termination of the EULA, as well as an obligation for the User (or the Customer, within whose sphere of responsibility the obligations fall as per the EULA) to compensate for any damages. It also constitutes a violation of the laws protecting intellectual property, authorship, patents, and industrial inventions.

7.5. The ownership rights regarding any software components necessary and/or useful for the operation of the software are specified in the additional and separate usage conditions that the User is required to accept if they intend to enjoy the full functionality of one or more of the Services. These conditions are not part of the EULA.

7.6. For specific content, different rights holders and/or usage terms may be indicated, which are distinct from those mentioned above.

7.7. ECS grants users the authorization to utilize the Resources, Connection Interfaces, ECS Content, Software, and Documentation to access one or more SaaS services.

7.8. Any other rights are expressly excluded and reserved.

8. Warranty of Full Ownership of the Software

8.1. ECS guarantees to be the owner of all rights (including, by way of example, copyright, related rights, sui generis rights, rights on trademarks, and, in general, industrial property rights, name rights, image rights, confidentiality rights, and, in general, personality rights) on the Software, documentation, and Updates, or to be legitimately authorized to grant the rights provided for in this EULA, having obtained the necessary authorizations from any third-party subjects who are the holders of these rights.

8.2. ECS therefore guarantees to the User that the granting of rights to the Software, documentation, and Updates, and their use, do not violate any third-party rights, and commits to indemnify and hold the User harmless from any third-party claims in this regard.

9. Warranty of proper functioning and correct implementation

9.1. ECS guarantees the proper functioning and the absence of major flaws and/or blocking defects in the Services, documentation, and Updates.

9.2. ECS guarantees that it will take all necessary measures to ensure the security of the Customer's data. In particular, ECS guarantees to update the Software and Updates according to the best market standards to protect the Resources, Software, and Updates from the risk of unauthorized computer intrusions, power interruptions or overloads, and any other risks, including natural disasters.

9.3. ECS guarantees that the Resources, Software, and Updates comply with current legal provisions regarding the processing of personal data and that they operate according to reasonable security standards.

9.4. ECS guarantees constant adjustments to the Resources, Software, and Updates to ensure compliance with the requirements stipulated by regulations issued throughout the duration of the EULA.

10. Indemnification

10.1. The User and/or the Customer agree to indemnify and hold ECS, its representatives, directors, employees, and its business partners harmless from any claims for compensation, including reasonable legal fees, brought by any third party:

a) arising from activities carried out by Users using the Software, Resources, or Services, or by any other person accessing the Resources using the User's Access Codes;

b) in connection with the Content that Users transmit using the SaaS Services.

11. Warranties

11.1. ECS undertakes an obligation of means and not of results.

12. Exclusion of Warranties

12.1. Subject to the explicit warranties provided under this EULA, ECS excludes any warranties.

12.2. The User acknowledges and agrees that no assurance, notice, or information sent orally or in writing by ECS to the User can create any form of warranty in favor of the User beyond those expressly provided for in the EULA.

13. Limitation of Liability

13.1. The User uses the Software, as well as the Resources and Services based on the use of the Software, at their own risk.

13.2. Notwithstanding the above, in no case shall ECS be liable to the User or any other party for loss of profit (loss of earnings or otherwise)

13.3. ECS shall not be liable for any damages incurred by third parties (indirect damages).

13.4. Nothing in these Conditions shall limit a Party's liability to the other Party resulting from willful misconduct or gross negligence on the part of that Party.

14. Personal Data Processing

14.1. The personal data, defined as "any information relating to an identified or identifiable natural person" ("Data Subject") of the Parties, for the purposes of accepting and executing the EULA, are processed in compliance with the provisions of data protection legislation (EU Regulation 2016/679 - the "GDPR" - and, where applicable, the Legislative Decree No. 196/2003 and subsequent amendments, especially following Legislative Decree No. 101/2018). This processing is also carried out in accordance with the measures issued by the Italian Data Protection Authority, the European Data Protection Board (EDPB, formerly WP29), and the best practices established in voluntary regulations on information security and protection.

14.2. The Parties mutually undertake to implement adequate measures (by way of example and not limited to) to maintain the confidentiality of Personal Data concerning each category of Data Subjects, to inform them properly about the processing, to ensure they can exercise the rights under Articles 15 to 22 of the GDPR, and to prevent unauthorized access to this data.

14.3. The Parties mutually undertake to:

a) observe the general principles of processing (accountability, lawfulness, fairness, transparency, accuracy, data minimization, purpose limitation, processing and storage limitation, integrity and confidentiality, data protection by design and by default);

b) provide the Data Subjects operating under the authority of the other party, if and as required, with information about the processing of Personal Data, identifying the appropriate legal basis for the processing along with supporting documentation demonstrating the choice (in cases of processing based on consent, legal obligation, legitimate interest, or public interest), and ensure their ability to exercise the rights under Articles 15 to 22 of the GDPR;

c) take appropriate measures (by way of example and not limited to) to maintain the confidentiality of Personal Data, prevent unauthorized access to them, and, in general, comply with all the obligations imposed on Data Controllers.

14.4. ECS has the authority to independently determine the purposes and means of processing information processed on behalf of the Customer that do not consist of Personal Data (properly de-identified in an irreversible manner) for the purpose of feeding protection heuristics related to the Services, even after the termination of the EULA.

15. Duration

15.1. The duration of the EULA (End-User License Agreement) begins when the User accepts the EULA and continues as long as the Client and/or User use the Software and/or Services.

16. Applicable Law and Competent Court

16.1. The EULA is governed by Italian law and, where directly applicable, by European law.

16.2. For any dispute arising from the validity, interpretation, or execution of this EULA, the exclusive jurisdiction lies with the Tribunal of Turin.

17. Miscellanea

17.1. Termination of EULA

a) ECS is authorized to assign the EULA, with all rights provided in the EULA, including the right to use the Content as stipulated in the EULA, to another entity that provides computer programs and similar services related to the Software and the Services.

b) The User may not assign or transfer the EULA or any of the rights, duties, or obligations under the EULA.

17.2. Complete Agreement and Modifications

a) The EULA supersedes any prior agreement, whether written or verbal, between ECS and the User concerning the subject matter of the EULA (except in the case of false statements made with willful misconduct or gross negligence), except for the Contract through which the Customer purchased the Software from the Reseller, the provisions of which condition the interpretation, validity, and effectiveness of the EULA. Any modification of the EULA will be binding only if documented in writing.

b) ECS may modify the provisions of the EULA, which will be published in the Dashboard and may be communicated via email; the modified provisions will also apply to Licenses already granted

17.3. Tolerance

a) The fact that ECS does not insist that the Customer and/or the User strictly adhere to the provisions of the EULA at all times, and/or does not exercise one or more of the rights established therein, does not result in the forfeiture of those rights or a waiver of the exercise of those rights by ECS.

17.4. Integration and Preservation

a) If one or more clauses of this EULA are or become contrary to mandatory legal provisions or public policy, they will be considered as not being in force and will not affect the validity of the other clauses of this EULA, except for the right of each party to request an amendment to those clauses.

b) If any provision of this EULA is deemed void or unenforceable by any Authority, that provision shall be deemed deleted from this EULA, and the remaining provisions of this EULA shall remain and continue to be fully valid and effective.

17.5. **Non-exclusivity of Remedies**

a) These rights and remedies are not exclusive but are in addition to other rights and remedies available under Applicable Law (including, but not limited to, injunctive remedies).

Signature for Acceptance of the End-User License Agreement (EULA)

____

ANNEX A – GLOSSARY

1. "**Access Codes**": the usernames and passwords assigned to the Customer by ECS.
2. "**Activation**": the operation through which the Customer (directly or through their delegate) first accesses it, activates the administrative account dedicated to the Services, and consults the related Dashboard.
3. "**Agent**": Software installed on the Users' devices that, by communicating with the SaaS Services, enables the operation of one or more Services.
4. "**Annexes**": the documents "Glossary" and "DPA", integral and substantial part of the EULA.
5. "**Applicable Fees**": the amount paid by the Customer to ECS for each minute the Services are made available. The calculation of Applicable Fees is performed as follows: a) amounts paid by the Customer to ECS for the provision of the Malfunctioning Service in the corresponding contractual year; b) divided by the sum of all minutes in the corresponding contractual year.
6. **"Applicable Regulations":** any provision, of any rank, belonging to Italian law or that of the European Union, in any way or to any extent applicable to the Contract and/or the Services, and in force at the time of its conclusion.
7. "**Authority**": a public or private entity or organization with administrative, judicial, police, disciplinary, or supervisory powers in any way related to the activities of the Data Controller.
8. "**Authorized Person**": the natural person placed under the direct authority of the Data Controller who receives instructions from the Data Controller regarding the Processing of Personal Data, in accordance with and for the purposes of Article 29 of the GDPR.
9. "**Certification Mechanisms**": the tools described in Article 42 of the GDPR.
10. "**Codes of Conduct**": the documents referred to in Article 40 of the GDPR.
11. "**Committee**" or "**EDPB**": the European Data Protection Board established by Article 68 of the GDPR and governed by Articles 68 to 76 of the GDPR, which replaced the WP29 on May 25, 2018.
12. "**Connection Interfaces**": interfaces (web, APIs, or other types) operating on certain configurations of certain devices through which Users' Agents can use the functionalities available on the SaaS Services.
13. "**Content**": text, images, audio and/or video recordings, data and/or information, including personal data, in any format (file or any other type of byte sequence) that is transmitted, copied, sent, and/or otherwise processed by the Customer and Users using the Services or by ECS and/or otherwise made available to the Customer, Users, and/or third parties.
14. "**Customer Domain**": an information system consisting of network-connected devices in use by the Customer.
15. "**Customer**": The organization or individual who (directly or through their representative) legitimately purchases the Software from ECS or its Resellers.
16. "**Dashboard**": A resource that provides the Customer with a visualization of information allowing the monitoring of events and activities related to the Services, accessible through the Access Codes.
17. "**Data Breach Notification**": the procedure provided for in Article 33 of the GDPR.
18. "**Data Breach Register**": the list of Data Breaches, maintained by the Data Controller and/or the Processor, in accordance with Article 33.5 of the GDPR.
19. "**Data Breach**": "A breach of security that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to personal data transmitted, stored, or otherwise processed," as defined by Article 4, paragraph 12, of the GDPR.
20. "**Data Controller**": "the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data," as defined in Article 4, paragraph 7 of the GDPR.
21. "**Data Processing Agreement**" or "**DPA**": The Data Processing Agreement as per Article 28 of the GDPR concluded between ECS and the Customer.
22. "**Data Processing**": "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction," as defined in Article 4, paragraph 2 of the GDPR.
23. "**Data Processor**": "the natural or legal person, public authority, agency, or other body that processes personal data on behalf of the data controller," as defined in Article 4, paragraph 1, no. 8, of the GDPR.
24. "**Data Protection Officer**" or "**DPO**": the individual or legal entity designated by the Data Controller in accordance with Article 37 of the GDPR, with roles and responsibilities defined by Articles 38 and 39 of the GDPR.
25. "**Data Retention**": The Data Retention period, set at 6 months from each individual Data Processing operation, after which the Data is either deleted or anonymized.
26. "**Data Subject**": "an identified or identifiable natural person," as defined in Article 4, paragraph 1, No. 1, of Regulation (EU) 2016/679 (GDPR).
27. "**Data**": one or more of the categories defined as Personal Data and Special Categories of Data.
28. "**Database**": Sets of data, uniform in content and format, made available by the Data Controller to the Data Processor in any way or form.
29. "**Designated Person**": a natural person, operating under the direct authority of the Data Controller, to whom specific tasks and functions related to the processing of Personal Data are assigned, in accordance with and for the purposes of Article 2-quaterdecies of the Privacy Code.
30. "**Director**": natural person with legal representation of one of the Parties.
31. "**Disclosure**": "the making Personal Data available to an indefinite number of persons, in any form, including by making them available or accessible," as defined in Article 2-ter, paragraph 4, letter b of the Privacy Code.
32. "**ECS**": Ermes Cyber Security S.p.A. con sede in Via Corso Bernardino Telesio n. 29, Torino (TO), CAP 10146, Italy, VAT and Tax Code 1171620019.
33. "**Employee**": an individual who performs work activities, regardless of the type of employment contract, under the authority of the Data Controller and/or the Data Processor.
34. "**Ermes for Enterprise**": a service that identifies the web threats to which Users' devices are exposed through the Agents that communicate with the SaaS Services in order to protect against identified web threats.
35. "**Ermes for MSP**": see "Ermes for Enterprise".
36. "**EULA**": this End-User License Agreement for Software use.
37. "**GDPR**": Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons concerning the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
38. "**Impact Assessment**": The activities defined by Article 35 of the GDPR.
39. "**License**": the license subject to the Contract, under which the User has the right to use a non-exclusive, perpetual, non-transferable, worldwide, non-free (costs borne by the Customer) license for the installation and use of the Software on devices as specified in the Contract through which the Customer purchased the Software, in compliance with all the terms and conditions outlined in ECS's General Terms and Conditions of Service.
40. "**Malfunctions**": availability issues and other malfunctions affecting the operation of the Services. Each of these malfunctions will also be referred to as a "Malfunction".
41. "**Notification of the Data Breach to the Data Subjects**": the process outlined in Article 34 of the GDPR..

42. "**Notification**": "making personal data accessible to one or more specified individuals who are not the Data Subject, the representative of the Data Controller in the Union, the Data Processor, or their representative in the Union, authorized persons under Article 2-terdecies for the processing of Personal Data under the direct authority of the Data Controller or the Processor, in any form, even by making it available, consulting it, or by interconnection" (as defined in Article 2-ter, paragraph 4, letter a of the Privacy Code).
43. "**Parties**": ECS, the Customer and/or the User.
44. "**Personal Data**": "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person," as defined in Article 4(1), Point 1 of the GDPR.
45. "**Prior Consultation**": the activities as provided for in Article 36 of the GDPR.
46. "**Privacy Code**": Italian 196/2003 Law Decree and subsequent amendments and/or integrations (in particular, Legislative Decree no. 101/2018).
47. "**Privacy Regulations**": Regulation (EU) 2016/679 ("GDPR"), Italian Legislative Decree No. 196/2003 and subsequent amendments and/or integrations ("Privacy Code"), as well as measures adopted by the Supervisory Authority in the execution of the tasks established by the GDPR and the Privacy Code, and other applicable regulations of any rank, including opinions and guidelines issued by the Committee.
48. "**Public Directories**": the directories of certified email addresses as per Article 16-ter of Legislative Decree 179/2012.
49. "**Recipient**": "a natural or legal person, public authority, agency, or another body to which Personal Data are disclosed, whether a Third Party or not," as defined in Article 4, paragraph 1, number 9, of the GDPR.
50. "**Register of Processing Activities**": documents whose contents are defined by Article 30 of the GDPR and, for Italy, by the FAQs of Garante della Privacy available at the URL https://www.garanteprivacy.it/home/faq/registro-delle-attivita-di-trattamento.
51. "**Regulations**" or "**Regulatory Framework**": one or more sets of rules referred to as Privacy Regulations and Applicable Regulations.
52. "**Representative**": "the natural or legal person established in the Union who, designated in writing by the data controller or processor in accordance with Article 27, represents them with regard to their respective obligations," as defined in Article 4, subparagraph 1, No. 17 of the GDPR.
53. "**Reseller**": the individual or legal entity that may sell ECS Software licenses to the Customer.
54. "**Resources**": systems consisting of software and data running on devices (physical or virtualized) in ECS's availability, accessible by the Customer and Users over the internet, which make the SaaS Services available.
55. "**Restriction**": "the marking of stored personal data with the aim of limiting their processing in the future," as defined in Article 4, paragraph 1, point 3, of the GDPR.
56. "**SaaS Services**": functionalities provided to the Customer using the Resources, including the functionality for recognizing and assessing web threats encountered by Users' devices.
57. "**Services**": individually or collectively, the Ermes for Enterprise Service, the Ermes for MSP Service, and the SaaS Services.
58. "**Software**": any set of instructions (programs and/or data) interpretable by a device to direct the operation of its processor, provided to the Customer and Users by ECS.
59. "**Special Categories of Data**": Personal Data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a person's sex life or sexual orientation, and personal data relating to criminal convictions and offenses or related security measures, as defined in Articles 4, 9 and 10 of the GDPR.
60. "**Supervisory Authority**": the independent public authority established by a European Union Member State or by the European Union itself, responsible for overseeing the application of data protection regulations (in Italy, the Garante per la Protezione dei Dati Personali, http://www.garanteprivacy.it).
61. "**Supplier**": the entity, whether a natural person or a legal entity, that submits a commercial offer to the Data Controller (irrespective of its acceptance by the Data Controller), as well as its directors, employees, and any agents.
62. "**System Administrator**": the entity defined and regulated by the General Provisions of the Italian Data Protection Authority (Garante per la Protezione dei Dati Personali), available on the website www.garanteprivacy.it, such as docweb no. 1577499 and 1626595.
63. "**Termination**": the dissolution of the Contract for any reason (including, by way of example, withdrawal and cancellation), even independently of the will of the Parties.
64. **"Third Party"**: any subject other than ECS, the Customer, and/or the User; in the context of the DPA, "the natural or legal person, public authority, agency, or any other body other than the data subject, the data controller, the data processor, and the persons who, under the direct authority of the data controller or data processor, are authorized to process personal data," as defined in Article 4, paragraph 1, no. 10 of the GDPR.
65. "**Updates**" refers to software updates provided by ECS to the Customer.
66. "**Users**": Those who use the Software from the devices of the Customer or their own on which the Software is installed, including the Customer itself if the Customer is an individual.
67. "**WP29**": the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established under Article 29 of Directive 95/46/EC, whose tasks are defined in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

ANNEX B - DATA PROCESSING AGREEMENT ("DPA")
ex art. 28 GDPR

between ECS and the Customer

GIVEN THAT

- In accordance with the EULA, ECS may come into contact with information that, within the context of the Customer's organization, consists of Personal Data related to individuals operating under the authority of the Customer (the "Users");
- In relation to such Data, the Customer acts as the Data Controller, whereas ECS acts as the Data Processor, as defined in the DPA;
- Article 4, paragraph 8, of the EU Regulation 2016/679 ("GDPR") defines the "Data Processor" as the "natural or legal person, public authority, agency, or other body that processes personal data on behalf of the Data Controller.";
- Article 28, paragraph 1, states that "Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject";
- Article 28, paragraph 3, specifies that processing by a processor must be governed by "a contract or other legal act under Union or Member State law that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, and the obligations and rights of the controller.";
- For the purposes of the Data Processing Addendum (DPA), terms with an initial capital letter shall have the meanings defined in the Glossary included in Annex A, where terms defined in the plural shall also be considered defined in the singular and vice versa;
- The Appendices are an integral and substantial part of the DPA.

All of the above being stated, the Parties agree as follows.

1. Statements of the Parties

1.1. The Data Controller, in light of the assessments conducted, acknowledges that the Data Processor has the necessary experience, capabilities, and reliability to ensure compliance with the provisions concerning the Processing, including the security aspects, and is, in any case, capable of providing sufficient guarantees to implement adequate technical and organizational measures in such a way that the Processing complies with the requirements of the Privacy Regulations and ensures the protection of the Data Subject's rights

1.2. The Data Controller declares:

a) to have chosen the Processor taking into account what has just been reported;

b) to authorize the Processor to entrust the other Processors indicated in Appendix C;

c) to be aware that the essential requirement for the use of the contractually agreed services with ECS is the compliance with the fundamental principles of Processing under Article 5 of the GDPR, to the extent within the Data Controller's competence, as well as the presence of a legal basis determining the lawfulness of the Processing of Personal Data, in accordance with Articles 6, 7, and 9 of Regulation (EU) 2016/679;

d) to be aware of their responsibilities regarding their role as the organization determining the means and purposes of Processing, including (by way of example but not exhaustively) the correct configuration and use of security features controlled by the Data Controller, taking into account the limited opportunity for ECS to intervene in the configuration of the information technology infrastructure used by the Customer;

e) to hold (where necessary) all the required authorizations from the Data Subjects to be able to process the Data, both independently and through ECS.

2. Object of the Agreement

2.1. The DPA governs the instructions provided by the Data Controller to the Data Processor for the purpose of Processing, as well as the terms, conditions, and mutual rights, obligations, and responsibilities.

3. Characteristics of Processing, Categories of Data and Data Subjects, Processing Instructions

3.1. The Processing subject to the Contract has the characteristics indicated in Appendix A.

3.2. The Data Processor carries out the Processing of the Data indicated in Appendix A, in relation to each Service. The Data Controller may inform the Data Processor of the information, among those indicated in Appendix A for each Service, that it does not intend to collect if necessary; for this purpose, it undertakes to send a written communication to ECS.

4. Rights of the Data Controller

4.1. The Data Controller has the right to:

a) monitor the actions of the Data Processor, with costs at their own expense;

b) object to changes (in addition and/or replacement with respect to Appendix D) to the list of other Data Processors for the performance of specific processing activities on behalf of the Data Controller, within 7 days since the notification by ECS;

c) communicate the cessation and/or suspension of the Processing if it is required by the need to comply with prohibitions or obligations arising from Privacy Regulations or Applicable Regulations, and/or orders/decisions of the Supervisory Authority or other Authorities;

d) recourse against the Data Processor for the amount, if any, paid as compensation for the damage suffered by the Data Subject, corresponding to the Data Processor's share of responsibility.

5. Obligations of the Data Controller

5.1. The Data Controller is obliged to:

a) Send a written communication to ECS if it does not intend to collect, through the Services, some of the information among those indicated in Appendix A for each Service;

b) carry out the Processing in compliance with Privacy Regulations and any other Applicable Regulations, in particular: - provide information to the Data Subjects on the processing of personal data in accordance with Articles 13 and 14 of the GDPR; - collect (where necessary) consent for data processing from Data Subjects; - ensure their ability to exercise the rights as per Articles 15 to 22 of the GDPR;

c) inform the Data Processor of the individuals appointed by them to carry out auditing and inspection activities, with a notice period of at least thirty days, and provide the qualifications and competencies of these individuals within the same timeframe to assess any potential conflicts of interest;

d) perform (and/or have performed) the activities mentioned in the previous point without interfering with the ordinary activities of the Data Processor;

e) promptly forward to the Data Processor any request from Data Subjects that involves the collaboration of the Data Controller, without undue delay;

f) make any necessary communication to the Supervisory Authority at the time of cessation;

g) promptly report to the Data Processor the occurrence of technical issues related to the Processing and the related security measures, which may pose risks of, including accidental, destruction or loss of the Data itself, or unauthorized access, or unauthorized or non-compliant processing with the purposes;

h) express any possible objections to the use by the Data Processor of one or more of the individuals listed in Appendix C, with a reasoned communication to be sent to the Data Processor no later than 10 days from the signing of the DPA;

i) make the first payment of any sums requested as compensation by Data Subjects to the Data Processor, with the right of recourse against the latter.

6. Rights of the Data Processor

6.1. The Data Processor has the right to:

a) receive adequate notice (of at least 15 days, unless there are reasons of justified and documented urgency) from the Data Controller regarding their need of performing checks, auditing activities, and/or inspections, as well as knowing the qualifications and competencies of the auditors within the same timeframe to assess any potential conflicts of interest;

b) promptly forward to the Data Controller any request from Data Subjects that may have been received;

c) process information that is not Personal Data even after the Termination, for the purpose of feeding heuristics for protection related to the Services;

d) recourse against the Data Controller for the portion of the amount, if any, paid as compensation for the damage suffered by the Data Subject, corresponding to the Data Controller's share of responsibility.

7. Obligations of the Data Processor

7.1. The Data Processor is obliged to:

a) carry out the Processing in accordance with the DPA and following any additional legitimate written instructions given by the Data Controller, if and to the extent that they are in compliance with Privacy Regulations and Applicable Regulations;

b) if required, provide the necessary cooperation to the Data Controller to allow them to provide Data Subjects with information regarding the processing of Personal Data in accordance with Articles 13 and 14 of the GDPR, as well as the collection of consent and its potential documentation (through the retention of paper documents, log files, and other electronic documents);

c) implement, taking into account the state of the art and the cost of implementation, all the most suitable and appropriate technical and organizational measures for the Processing to ensure its security, considering all aspects of the Processing and, in particular, the risk to the rights and freedoms of the Data Subjects, with specific reference to what is indicated in Article 32 of the GDPR;

d) list in Appendix B the security measures in use;

e) specify the other Data Processors in Appendix C and bind them to obligations that ensure at least the same level of Data protection as provided in the DPA;

f) instruct Authorized Personnel and/or System Administrators on the need to respect confidentiality and the prohibition of Communication and/or Disclosure of Data, and provide them with written instructions in compliance with the Regulations, and oversee their actions;

g) promptly inform the Data Controller of Personal Data Breaches (where confirmed as such following an internal investigation) of which it become aware, concerning the systems directly related to the provision of the Services;

h) delete Personal Data (and any existing copies) at the time of Termination, subject to the option described in the subsequent Article 8.2.f with respect to information that is not Personal Data;

i) provide the Data Controller with the fullest cooperation for the purpose of complying with obligations imposed by Applicable Regulations that are closely related to the execution of the EULA, such as (by way of example), those related to security, the maintenance of the Registry of Processing Activities, the execution of Impact Assessments, Data Breach Notification, Data Breach Communication to Data Subjects, and Prior Consultation;

j) collaborate with the Data Controller in implementing any instructions possibly issued by a Supervisory Authority in any way or to any extent relevant to the execution of the EULA and/or the DPA

k) provide the widest cooperation to the Data Controller for the purpose of responding to requests from Data Subjects that involve the acquisition of information in the possession of the Data Processor;

l) indemnify and hold the Data Controller harmless from any liability, direct or indirect damages, claims, penalties, costs, expenses (including legal fees and expenses), loss of profits resulting from non-compliance with the instructions provided by the Data Controller and/or any unlawful Data Breaches and Data Processing carried out by the Data Processor, authorized persons for processing, or its employees, personnel, consultants, or subcontractors. For this purpose, the Data Processor shall enter into and/or maintain adequate insurance coverage to cover all damages that may be caused to the Data Controller and/or their affiliates and/or companies controlled by them as a result of the Data Processor's breach of the obligations specified in the DPA and the obligations provided by applicable laws and regulations on Data Protection.

8. Empowerment of the Parties

8.1. The Data Controller is empowered to:

a) communicate to the Data Processor which information, among those indicated in Appendix A for each Service, the Data Controller does not intend to collect, and, for this purpose, send a written communication to ECS;

b) request the cooperation of the Data Processor, where possible and taking into account the nature of the Processing, in activities related to the Data Controller's obligation to respond to requests for the exercise of rights made by Data Subjects in accordance with Privacy Regulations;

c) make use of other Data Processors in relation to the Data and/or Data Processing activities that are similar to those necessary for the execution of the EULA.

8.2. The Data Processor is empowered to:

a) resort to other entities in the execution of the Processing; the Data Processor, for this purpose, will inform of any changes regarding the addition or replacement of entities to which the execution of the Processing is entrusted, thus giving the Customer the opportunity to object to such changes, which will be deemed approved in the absence of explicit opposition within 7 days from the communication, provided that they are communicated to the Data Controller in advance with a notice period of 15 days;

b) reserve the right to charge the Data Controller for the costs and expenses incurred for controls, auditing activities, and/or inspections, should they result from deficiencies on the part of the Data Controller recognized as such by both parties in relation to the obligations established by Applicable Regulations or non-compliance with the EULA or the DPA, provided that they are communicated to the Data Controller in advance with a 15-day notice;

c) transfer (through Communication, transmission, and/or making available) Personal Data, directly and/or through another Data Processor (indicated in Appendix D or subsequently identified and approved by the Data Controller), even outside the European Economic Area or to an international organization, ensuring in any case compliance with the guarantees or derogations provided in Chapter V of the GDPR and giving advance notice to the Data Controller, who, in the absence of a response within 30 days of the notification, authorizes the transfer;

d) inform the Data Controller if the legislation of the State of origin requires the transfer of data outside the European Economic Area unless such information is prohibited by the law for substantial reasons of public interest;

e) notify the Data Controller of the deletion of any Databases at the time of Termination, without prejudice to the right to retain, for the purpose of feeding heuristics for protection associated with the Services, information from which they are unable to re-identify the Users;

f) retain Data in anonymous form for the purpose of study, statistics, and research once the Data Retention period has elapsed, in accordance with Article 89.1 of the GDPR.

8.3. Each Party has the option to adhere to Codes of Conduct and/or Certification Mechanisms, with the effects provided for in Article 28.5 of the GDPR.

9. Obligations of the Parties

9.1. The Parties mutually undertake to:

a) provide, upon request, the contact details of the Data Protection Officer and the Representative, if appointed by each Party;

b) inform the other Party of any requests, orders, or checks by one or more Authorities from subjects authorized and/or delegated by them (by way of example, the Judicial Authority of any country in the world) in any way relevant to the execution of the EULA and/or the DPA;

c) promptly inform the other Party of any circumstances that may prevent from fulfilling the obligations under the DPA.

10. Effects of Termination

10.1. In the event of Termination (for any reason other than a breach by the Customer of its obligations), all Personal Data will be deleted by the Data Processor, except for the latter's option under Article 8.2.f. with respect to information that is not Personal Data.

11. Other Provisions

11.1. The relationships between the Data Controller and the Data Processor with regard to the Processing of Personal Data are governed as indicated in the DPA; any concession or practice that departs from the above-mentioned regulation shall not be considered as modifying the relationship, which is therefore exclusively governed by the DPA.

11.2. For matters not expressly provided for, reference is made to the Applicable Regulations.

DPA Appendices:

A. Categories of Data Subjects and Personal Data processed by the Data Processor

B. Security measures implemented by the Data Processor

C. List of Other Data Processors

APPENDIX A - Categories of Data Subjects and Personal Data processed by the Data Processor

ECS will perform the Processing with the characteristics indicated below in relation to each provided Service.

1. ERMES FOR ENTERPRISE / FOR MSP

1.1. The Processing has the following characteristics:

a) Mode: computerized;

b) Purpose: protection against web attacks for individuals operating under the authority of the Customer;

1.2. The categories of Data Subjects are Users ('those who use the Customer's devices on which the Customer has installed the Agent to enable the functionality of the Ermes for Enterprise Service').

1.3. The information processed is as follows:

a) HTTP traffic logs consisting of the following data:

- Timestamp of HTTP request
- Method of HTTP request
- Hostname extracted from the URL
- URL requested
- User agent
- Header HTTP
- Cookie
- Identifier of the request within the browser session
- Flag set to 1 if the request has been generated by a direct interaction of the user, 0 otherwise
- Web page from which the request was generated
- Browser from which the request was generated
- Mobile app from which the request was generated
- Tags defined by ECS and associated to the request which has been blocked
- User who generated the request
- Device from which the request was generated

b) Information related to browser extensions installed on the devices used by Users:

- Identification Data describing the extension (identifier, name, description, version, homepage, update URL, permissions required)
- Timestamp of the moment when the extension installation was identified
- Browser on which the extension installation was identified
- Activation status of the extension
- Kind of installation of the extension
- User associated to the extension installation
- Device on which the extension installation was identified

c) Only for events of prohibited use of corporate accounts (module "Business Account Protection"), based on the policies defined by the Customer:

- Timestamp of the event of blocked use of the corporate account
- Hostname of the web page on which the unauthorized use of corporate account was blocked
- Browser on which the unauthorized use of corporate account was blocked
- Corporate account used by the User
- Identifier and name of the input form field in which the User used the corporate account
- User for which the unauthorized use of corporate account was blocked
- Device on which the unauthorized use of corporate account was blocked

d) Only for events of prohibited use of corporate data (module “Data Loss Prevention”) based on the policies defined by the Customer:

- Timestamp of the event of blocked use of the corporate data
- Hostname of the web page on which the unauthorized use of corporate data was blocked
- Browser on which the unauthorized use of corporate data was blocked
- User for which the unauthorized use of corporate data was blocked
- Device on which the unauthorized use of corporate data was blocked

e) Technical cookies strictly necessary for the authentication of the User's device and the operation of the Service.

1.4. Duration (Data Retention period): the information mentioned in the previous point 1.3.a, not being Personal Data, will be retained even after Termination for the purpose of feeding the heuristics of protection connected to the Services; Personal Data processed in the execution of the Service (1.3.b, 1.3.c, and 1.3.d) will be deleted once the Data Retention period has elapsed.

APPENDIX B - Security measures implemented by the Data Processor

ECS adopts the technical and organizational security measures detailed below to ensure an adequate level of security in relation to the risk (taking into account the risks of destruction, loss, alteration, unauthorized disclosure, or access, whether accidental or unlawful):

- **PHYSICAL**
  - Day/night surveillance agency
  - Internal alarms
  - Perimeter alarms
  - Mobile safety deposit boxes
  - Sealed and sealed documentation (if necessary)
  - Fire extinguishers
  - Emergency lighting
  - Fixed fire-fighting systems
  - Fire doors
  - Emergency response with external company
  - Locks on cabinets and drawers
  - Office locks
  - Air conditioning systems
- **IT**
  - Anti-malware
  - Authentication
  - Multi-factor Authentication
  - Authorization (access privileges)
  - Backup
  - Business continuity Plan
  - Encryption of data at rest
  - End-to-end encryption for communications
  - Multi-channel sharing of data protected with passwords
  - Disaster recovery Plan
  - Hardware firewall
  - Log management
  - Password Management System
  - Periodic penetration tests
  - Pseudonymization
  - Geographic data redundancy
  - Remote data wipe
  - Logic separation of data
  - VPN (Virtual Private Network)
- **ORGANIZATIONAL**
  - Role-based access control
  - Data Processing Agreements (DPAs) with subprocessors
  - Adoption of compliant storage systems
  - ISO27001 data security certification
  - Appointment of System Administrators
  - Dedicated communication channels (e.g., specific email address)
  - Third-party auditing
  - Instructions to authorized personnel and designates
  - Training
  - Internal auditing checks
  - Physical separation of environments
  - Privacy consulting by an external entity for support
  - Data breach management procedures
  - Regulations or policies for the use of company devices

APPENDIX C – List of Other Data Processors

Name	Type of service provided to ECS	Service from ECS using the provided service		Data Processor established outside of EU (Yes / No)
		Ermes for Enterprises	Ermes for MSP	
Amazon Web Services	Cloud Infrastructure	X	X	Yes *
Google Cloud Italy S.r.l.	Geolocation APIs			Yes **
	Installation identifiers Execution traces Breakpad minidump	X	X	
Bugfender	Interactions with Service Unexpected failure data Performance data Other diagnostic data Device identifiers	X	X	No
MongoDB Inc.	Storage of collected data	X	X	Yes ***
Auth0 Inc. (Okta Inc.)	Authentication data		X	Yes ****

*** Additional documentation and assurances provided by AWS:**

1) https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf;
2) https://d1.awsstatic.com/Processor_to_Processor_SCCs.pdf
3) https://d1.awsstatic.com/whitepapers/Security/navigating-compliance-with-eu-data-transfer-requirements.pdf
4) https://d1.awsstatic.com/Supplementary_Addendum_to_the_AWS_GDPR_DPA.pdf.

**** Additional documentation and assurances provided by Google:**

1) https://cloud.google.com/terms/sccs
2) https://cloud.google.com/terms/data-processing-addendum
3) https://services.google.com/fh/files/misc/safeguards_for_international_data_transfers_with_google_cloud.pdf

***** MongoDB Documentation:** https://www.mongodb.com/legal/dpa

****** Additional documentation and assurances provided by Auth0 Inc. (controlled by Okta Inc.):**

1) https://www.okta.com/trustandcompliance/