# License Agreement ZAIUX Evo

**Software: ZAIUX Evo**
**Vendor: Pikered S.r.l.**
**Version: v.1.14**
**Subject: Personal, limited and non-transferable license of the right to use ZAIUX Evo**
**Date: 12.03.2026**

## 1. Terms and conditions of license

1.1. The exclusive, personal, and non-transferable right to use the Software, as defined below, for the duration of this license agreement is subject to the user's acceptance of these terms and conditions, as well as the License Acceptance Form to which these terms and conditions are attached (altogether, the "**Agreement**").
1.2. This Agreement is intended for users acting for professional purpose only. By entering into this Agreement and /or launching the Software, you declare and warrant that you are not a private consumer.
1.3. The Client and/or his legal representative must be at least 18 years of age and must have attained the age of majority according to the law of his state of legal residence. If this Agreement is signed on behalf of a company, it is necessary to be duly authorized to represent the company and accept the terms and conditions of this Agreement on behalf of the Company. By entering into this Agreement and/or using the Software, the Customer represents and warrants that he meets all requirements necessary for entering the same and/or for using the Software.
1.4. The use of the Software is subject to the acceptance of this Agreement. The agreement is intended to be released for the period mentioned in the Sales Terms and in the License Acceptance Form Contratto, for the aspects that may require further detail compared to what is mentioned in the Sales Terms. A valid company email address must be provided to use the Software and services provided under this Agreement.
1.5. Access to the Software is granted with a personal and non-transferable license by the Vendor (as defined below). The Software may be used within the limits and in accordance with the terms and conditions of this Agreement.
1.6. The interface of the Software will be exclusively in English.

## 2. Definitions

2.1. Customer – subject that signs this Agreement whose details are specified in the License Acceptance Form.
2.2. Sales Terms- the contractual terms signed by the Customer for the purchase of the Software and which may be concluded, depending on the circumstances, with the Vendor or with authorized distributors of the Vendor.
2.3. User - natural person who, as part of the Red Team, uses the Software on the instruction and under the responsibility of the Customer.
2.4. Maintainer User– User with full access to all the Software functionalities and to all the Vendor's technical communications, who is mentioned in the Sales Terms and in the License Acceptance Form or also enabled by another Maintainer User.
2.5. Software - the set of components and applications of ZAIUX Evo as described in clause 6 of this Agreement and according to the specifications provided in the Technical Datasheet.
2.6. Pay As-You-Go License – Agreement that stipulates the Customer's right to use the Software according to the final count of the Tokens actually used on a monthly basis, possibly setting a maximum number of usable Tokens.
2.7. Pay-in-Advance License –Agreement that stipulates the Customer's right to purchase a determined number of Tokens, that can be used within a certain validity period.
2.8. Pay-in-Advance - Flat License – Agreement which stipulates, in return for payment of a fixed fee mentioned in the Sales Terms, the Customer's right to use the Software for multiple performances limited to the Customer's organization and within the limits of normal use of the Software as determined by the Manufacturer on the basis of the Customer's type for the duration of the Agreement.
2.9. Token – virtual unit corresponding to a single execution of the Software within the period specified in the Agreement.
2.10. Red Team - group of Users who, as ethical hackers, attack the Target Infrastructure to verify/validate its resilience of the defensive solutions set up and acting on the instructions of the Customer. It may be composed of one or more members within the Customer's organization.
2.11. License Acceptance Form – Form that specifies all the information regarding the Agreement and which is not specified in the same, as well as the Customer's email contact.
2.12. Vendor or Pikered - Pikered S.r.l., VAT: IT 11458640965, with registered office in Via Borgonuovo, 9, 20121 Milano (MI), e-mail address: info@pikered.com, which has developed the Software and which is owner of all Software's rights, including intellectual property rights
2.13. Target Infrastructure - the IT infrastructure on which the Software activity will be conducted, to test its resilience and ability to resist cyber-attacks; it is owned by the Customer or third parties who have authorized the Customer to use the Software on their computer infrastructure.
2.14. Technical datasheet - accompanying technical documentation of the Software.

## 3. Subject of the Agreement

3.1. This Agreement governs the right to use the Software; pursuant to the Agreement, the Manufacturer grants the Customer a non-exclusive, non-transferable and revocable license for the time established in clause 9 to use and to let Users use the Software, as well as its Technical Datasheet ("**License**") under the terms and limits provided by this Agreement. The Customer guarantees, also pursuant to art. 1381 of the Italian Civil Code, that the use of the Software abides by this Agreement. The Software will remain the exclusive property and availability of the Vendor, who is the sole holder of the economic exploitation.

3.2. The Vendor and its subcontractors shall each be the owner and holder of their respective rights in trademarks, trade secrets, patents and any other additional copyright and intellectual property rights on the Software, applications, services and documents. Therefore, all rights not expressly granted in this Agreement remain with them.

3.3. The Customer declares and acknowledges that he has not taken part in any way in the development of the Software and applications, thus renouncing to claim any right on them.

3.4. The License is released on a non-exclusive, non-transferable basis for the sole purpose of testing, typically by a Red Team, the security status of the Target Infrastructure.

3.5. This Agreement does not include, unless specifically agreed in writing in the Sales Terms, any project management activities, risk assessment activities and the use of any support or consultancy activities that do not relate to the Software, as well as any activity on different operating systems, system software and applications.

3.6. The use of the Software and of its software and application components represents a non-transferable right, not even for business purposes. This right is limited to the sole purpose of testing the security status of an IT infrastructure owned by the User, by the Customer or by the Company that has authorized the User and/or the Customer to use the Software, and in any case always for ethical purposes.

## 4. Consideration

4.1. The Customer shall pay to the Vendor, or to the person otherwise appointed in the Sales Terms, the consideration agreed in the terms and in the manner therein specified.

4.2. In case of Pay-in-Advance Flat License, the Manufacturer reserves the right, in case it detects a use of the Software abnormal compared to the use considered normal for the type to which the Customer belongs, to verify the absence of anomalies in the permitted use of the Software and, in the case of applying rates provided for other types of Licenses. In such case, the Vendor will notify the Customer of the abnormal use and of the rates that will be applied subsequently, without prejudice to the Customer's right to communicate the withdrawal from the Agreement within 30 days following receipt of such communication. In any case, the Producer has the right to terminate the Contract pursuant to article 1456 of the Italian Civil Code whenever the abnormal use is due to a use of the Pay-in-Advance Flat License at third party Target Infrastructures in violation of the terms of the Pay-in-Advance Flat License.

4.3. Should the agreed consideration not be paid in full within the above-mentioned time limit, the Vendor reserves the right to charge additional default interests on the due amount, which are calculated from the invoice date and for each subsequent day until the full balance of the sum by the Customer, at the rate set in art. 2, para. 1e, and art. 5 of Legislative Decree no. 231/2002. The Customer will also be responsible for all legal and collection costs incurred by the Vendor to collect the amount due by the Customer, as well as compensation for any damage.

## 5. Obbligations of the Customer

5.1. By accepting this Agreement, the Customer undertakes not to lease, rent, grant in use and sub-license the Software, or use components of the Software separately. In addition, the Customer undertakes not to perform any reverse engineering, decompile, modify, translate, disassemble, display source code, or create derivative works from any part of the Software. The Customer agrees and undertakes not to allow, also under art. 1381 of the Italian Civil Code, to third parties to benefit from the use of the Software or features of the Software through timesharing, office services and other arrangements. The Customer also agrees not to upload the Software, or any information or other elements related to the Software on websites and databases for the collection, identification, and analysis of malware such as, but not limited to Virustotal, Hybridanalysis, Malpedia.

5.2. The Customer will use the Software only in ways that are lawful and permitted by applicable Law and undertakes not to encourage any behavior that is contrary to applicable Law too. Purely by way of example, the Customer will not use or encourage the use of the Software for any activity that would constitute a criminal offence or that would otherwise interfere with the use and enjoyment of the Software by others or use the Software to track or monitor the location and activities of any individual, in the absence of the required legal authorizations.

5.3. The Client undertakes to comply with and enforce for Users all obligations of this Agreement, as well as the legal provisions, regulations, rules and disciplines (including applicable contracts and collective agreements) that are in any manner related to the performance of the Agreement, including with regard to criminal law on unlawful access to information systems, as well as on hiring of labor, insurance, social security and rights of the workers, remuneration, compulsory contributions, including salary contributions, severance pay, social security contributions and insurance premiums, safety measures (including the safety measures referred to in Legislative Decree n. 81/2008, and following modifications), and any necessary authorizations from the competent authorities. Therefore, Users may not claim in any way an employment relationship, or any other kind of right, against Pikered.

## 6. Software features

6.1. The Software is an advanced Full Cloud (SaaS) solution that automates Command and Control (C2) attack activities on IT infrastructures, such as Red Teaming, Breach & Attack Simulation, Ransomware Simulation and Active Directory Health Check, Able to generate reports free of false positive and with a complete Remediation Plan in reference to the MITRE ATT&CK® framework.

6.2. The Software is composed of the following components:

- A component that can be classified as malware (this component is executed within the Target Infrastructure)
- A component of Artificial Intelligence DPZR™ Engine Sandbox, to build and plan Command & Control activities.
- A user interface component ZAIUX Evo Portal, to manage the user profiles and browse the output generated in html or JSON format.

The Customer is solely responsible for launching the Software.

6.3. Data Accessibility. Any information owned by the Customer stored in the Target Infrastructure will not be available to the Vendor. At the end of the Agreement, any information resulting from the Breach & Attack Simulation will be automatically and permanently deleted and cannot be retrieved by the Customer unless it is saved on its systems during the term of the Contract. The only exceptions are final reports, which will remain accessible locally from the web interface of the Software.

6.4. Attacks performed by the Software. The Breach & Attack Simulation performed by the Software includes different types of cyber-attacks. The aim is to highlight the vulnerabilities of the Target Infrastructure represented in the report generated as output at the end of execution, based on the MITRE ATT&CK® framework, which highlights possible mitigation actions regarding these vulnerabilities.

6.5. The Customer remains solely responsible for the security of the IT infrastructure on which the Software is used. The Vendor cannot be held responsible for any unauthorized or authorized access to the Target Infrastructure by third parties, as a result of the use of the Software and the Customer will indemnify and hold Pikered harmless from any harmful consequences produced to third parties resulting from the use of the Software.

6.6. Here follows a list of features of the Software, as a reference (and non-exhaustive), which may be subject to constant changes and updates. Further information is available at the following link: https://attack.mitre.org/techniques/enterprise. The execution by the Software of all attacks mentioned is not guaranteed.

6.6.1. EDR/XDR Evasion out-of-the-box
6.6.2. C2 communication via HTTPS + SMB Pivoting
6.6.3. AD Health check
6.6.4. Ransomware Simulation
6.6.5. Lateral Movement
6.6.6. Privilege Escalation
6.6.7. In-Process .NET Assembly execution
6.6.8. Active Directory misconfiguration leveraging

In case of a *trial*, the Customer will have the right to use a single Token with limited features and generation of the related report, limited as appointed in the Sales Terms or in any case in written form.

6.7. **Disruptions and effects of the Software execution** - Disruptions in the functioning of the Target Infrastructure may occur, due to both the activity of the Software and to a reaction of the installed computer defense systems. The defense systems and the resulting reactions will not be communicated in advance and will not be known or evaluated by the Vendor. The Customer acknowledges that it is its sole responsibility to assess the possible consequences of running the Software on the Target Infrastructure and that the Vendor will not be responsible for any disruption in the functioning of the Target Infrastructure or of other computer systems owned by the Customer or third parties, as a result of using the Software.

6.8. **Assumption of liability by the Customer**: By using the Software, the Customer understands and agrees that the risks described above may occur and must be assessed in advance by the Customer. It is the Customer's responsibility to use the Software consciously and with the required technical expertise, including, where appropriate, with the involvement of the necessary specialized personnel (such as, for example, the IT manager and the System Administrator of the Target Infrastructure). It is possible to stop running the Software and take any necessary action to restore normal network operation and services that may be compromised. To this aim, the intervention of the Vendor is not necessary, nor can it be required; Pikered does not provide such service, which is not included in this Agreement. The Vendor disclaims all liability for the occurrence of the risks described above and in general for any risks arising from using the Software. Pikered reserves the right to sue the Customer for any damage arising from the use not permitted or not in accordance with this Agreement.

6.9. **Assistance** – In case of malfunctioning (e.g. user interface malfunctioning, anomalies in execution, crash), the Customer is entitled to make a report using the dedicated support feature in the Software Dashboard. Following the report, Pikered undertakes to take charge of the report ticket within the next working day. After taking charge, Pikered may need to acquire additional information to classify the ticket Pikered will, at its sole discretion, classify the report as "unexpected behavior" or as a "bug". If the report is classified as a "bug", Pikered undertakes to resolve it, in a reasonable time, through modifications to the Software. Such support is guaranteed for the whole Software life cycle. During the ticket management, progress and closure notifications related to the same are provided.

6.10. The Customer acknowledges that any improvement, new functionality or in general any modification of the Software that should result from reports, suggestions or in general interactions of any kind with Pikered will be considered an integral part of the Software, on which the Vendor retains all rights specified in the Agreement.

6.11. Pikered does not guarantee any features or results other than those described in this section.

## 7. Technical requirements

7.1. The correct functioning of the Software and of all its components is guaranteed only when the Target Infrastructure meets the following requirements:

7.1.1. Microsoft Windows 10/2016 or higher, 64-bit only and in Microsoft Active Directory environments.
7.1.2. Linux, 64bit only and in Microsoft Active Directory environments.

7.2. The hardware requirements are those stated by Microsoft for the above operating systems.

## 8. Updates and unilateral modifications

8.1. The Software requires updates to function properly. Updates may be bug fixes or new models, new categorizations, definitions or rules for control elements and minor development of software, applications or accompanying documents. Software updates will be made available and used during the validity period of the license version under the terms of this Agreement between the parties. Any changes to the Software are subject to the terms and limits of this Agreement and to additional terms which may be required to be accepted when updating.

8.2. The release of new versions of the Software may require acceptance of additional general contract terms. In this case, the possibility to update the Software and use it in its most up-to-date version is subject to the acceptance of these additional contract terms. Unless expressly stated in the additional general contract terms, this Agreement shall remain in force.

8.3. The updates will replace Software parts that were previously included in the version. Pikered undertakes to notify significant changes to the Software or this Agreement by sending an email to the address appointed in License Acceptance Form. The Vendor also undertakes to inform of significant modifications to the Software, as well as possible disruptions needed to make these updates available, by sending an e-mail to the addresses associated with the Maintainer Users.

8.4. For security, update and maintenance reasons too, Pikered reserves the right to modify the Software and each of its features or components at any time.

8.5. Pikered undertakes no obligation to (i) provide updates, (ii) continue to provide or enable specific features and/or functions of the Software, or (iii) ensure the functioning of obsolete versions of the Software. In addition, the Customer agrees that all updates are (i) considered part of the Software, (ii) subject to this Agreement and (iii) necessary for the proper use and functioning of the Software. To ensure the functionality and security of the Software, the Customer declares to have understood that the Software may be interrupted or suspended due to maintenance activities, revision, update, migration, improvement and security that may be necessary or appropriate.

8.6. Except as provided in clause 8.1 above, Pikered reserves the right to amend this Agreement by giving reasonable prior written notice to the Customer. The Customer shall have the right to withdraw from this Agreement within 30 days of receipt of notice of amendment to the Agreement.

## 9. Duration

9.1. In the case of a Pay-in-Advance-Flat License, this Agreement shall run for 12 months from its conclusion, unless otherwise stated in the Sales Terms and in the License Acceptance Form, for those aspects that require further detail than appointed in the Sales Terms. In case of a Pay-As-You-Go License, this Agreement has a duration of 12 months from the last invoice issued, unless otherwise stated in the Sales Terms and the License Acceptance Form, for aspects that require further detail than appointed in the Sales Terms.

9.2. In the case of a Pay-in-Advance License, this Agreement is valid until the validity of the purchased Tokens. Unless otherwise specified in writing, the validity period of the Tokens is 12 months from the date of purchase. In case of purchase of additional Tokens before the expiration date of the remaining and still unused Tokens, the duration of these Tokens is renewed by another 12 months. Throughout the validity period of the Tokens, the Customer will have the right to use updates that in turn will be automatically applied to the Software by the Manufacturer from time to time. The components of such updates will be considered integral parts of the Software.

9.3. During the License validity period, Pikered will provide updates to the Software until the end of its life at the sole discretion of Pikered. In the event of the end of the Software's life, Pikered will notify the Customer by sending an e-mail to the address appointed on the Order Form.

## 10. Dual use

10.1. The Customer acknowledges and accepts that the Software is classified as dual use product pursuant to EU Regulation 2021/821, category 4D004.

10.2. The Customer undertakes to allow the usage of the Software exclusively to users within the European Union and not to export, transfer, resell or supply, either directly or indirectly, the Software to subjects residing outside the European Union without prior obtainment of all the necessary authorizations.

## 11. Limitation of liability and indemnification

11.1. Pikered guarantees that it has the power and authority to license the Software to the Customer. Except for the warranty herein stated, the Software is provided "AS IT IS" and Pikered declines all other warranties, express or implied, including without limitation any implied warranties of merchantability, performance or fitness for a particular purpose. Pikered does not guarantee that the use of the Software by the Customer will be free from errors.

11.2. By agreeing to use the Software, the Customer declares that it understands the possible consequences of running the Software on the Target Infrastructure. The Customer also accepts the possible malfunctions and consequences described, by way of example but not exhaustive, in section 6 of this Agreement, exempting Pikered from any liability.

11.3. Pikered or its sub-suppliers shall not be liable in any way to the Client or third parties on whose Target Infrastructure the Software is used (i) for any loss or damage arising from the performance of the Software and the attacks described in this Agreement, (ii) for damages resulting from the interruption of activities and potential economic loss arising from the performance of the Software, or (iii) for any loss or consequence arising from using the Software.

11.4. These limitations will also apply in the event that Pikered is aware or has been warned that such damage was possible, regardless of the source of the warning, whether contractual, from Software liability, non-contractual or any other nature. By using the Software, the Customer accepts the risk that the Software may be used by third parties who fraudulently access the Target Infrastructure, without any liability on the part of Pikered.

11.5. The Customer undertakes to indemnify Pikered from any liability arising from failure of the Customer to comply with clause 10.2.

11.6. Without prejudice to the foregoing, Pikered's liability arising directly or indirectly from this Agreement shall in no event exceed the value of the consideration paid to Pikered for the use of the Software under the Agreement.

11.7. For the entire duration of the Agreement and even after dissolution or termination of its effectiveness due to any cause, the Customer shall indemnify, hold harmless and compensate Pikered, without any limitation, from any detrimental consequence arising for it from failures and non-compliance with legal and contractual obligations attributable to the Customer and/ or Users.

## 12. Personal Data Protection

12.1. The use of the Software may be subject to laws and regulations on personal data protection. Pikered will process the personal data listed below in compliance with the EU Regulation 2016/679 of the European Parliament, of the Council of 27th April 2016 and subsequent amendments and updates.

12.2. To use the Software and operate the Software, Pikered acts as data controller for the processing of the following data: Personal data (of the User and the Customer) necessary to create the customer registry and to manage the authorization process to use the Software and to subsequently manage the License.

12.3. Data processing has the sole purpose of providing the Software. Personal data will also be processed for the purpose of executing an Agreement of which the interested party is part, solely and exclusively for performing the services provided under this Agreement, to comply with the tax and accounting obligations and to comply with the obligations under current legislation.

12.4. Pikered collects personal data for the purpose of managing the Software license. The following identification data will be processed such as: name, customer identification number, telephone number, e-mail and registration number. The processing of personal data is necessary for Pikered to fulfil its obligations towards the Customer, in accordance with the Agreement.

12.5. The personal data of third parties provided, under the Agreement, will be processed by Pikered only as authorized party to process such data, as required, to provide services or fulfill obligations under this Agreement. For such data of third parties, the Customer guarantees following: it is authorized to process the data and transmit them licitly to Pikered, in accordance with applicable law, and it has properly informed the interested parties and obtained their consent where necessary. In any event, the Client agrees to indemnify and hold harmless Pikered for any harmful consequences that it may suffer due to failure to comply with the above.

- 12.5.1. In accordance with art. 15 and following of Regulation EU 2016/679, the interested party has at any time the right to: Ask for confirmation of the existence or not of his personal data and make it available to them in an intelligible form.
- 12.5.2. Request and obtain from the data controller access to personal data, updating and rectification or deletion of the same, or restriction of processing that concerns it; the interested party has equally the right to object to the processing of data in addition to the right to data portability.
- 12.5.3. Obtain information about the purposes and methods of processing, categories of personal data, recipients or categories of recipients to whom personal data has been or will be communicated and, where possible, the retention period.
- 12.5.4. Obtain the portability of data, that is to receive them from the data controller in a structured format, commonly used and readable by an automatic device, and transmit them to another controller without hindrance.
- 12.5.5. Object at any time to the processing.
- 12.5.6. Withdraw consent at any time without affecting the lawfulness of processing, based on the consent given prior to withdrawal.
- 12.5.7. Address all communications to the data controller, Pikered, via the following email address: dpo@pikered.com.
- 12.5.8. Lodge complaints to the supervisory authority (Italian Data Protection Authority – www.garanteprivacy.it).

12.6. Limited to the support activities provided for in this Agreement, Pikered may process information (including personal data) of the Customer. In this case, Pikered may process such information within the limits of what is appointed in Annex [A] to this Agreement, which contains the Data Processing Agreement.

12.7. ELECTRONIC COMMUNICATIONS: Pikered may need to send legal or other communications relating to the Software, Subscription Services or Pikered's use of the information provided in the execution of this Agreement ("Communications"). Pikered will send the communications by email to the address provided in the License Acceptance Agreement or will post them on its website at www.pikered.com. By accepting this Agreement, the Customer further acknowledges and confirms that it can access the Communications on the website www.pikered.com.

## 13. Confidental Information

13.1. During the negotiations for the conclusion of the Agreement and the performance of what is stipulated therein, the parties have exchanged and will exchange certain technical, financial, commercial, managerial, administrative, legal and economic data and information (including, without limitation, each party's intellectual property as well as information, data, know-how, specifications, drawings, design, software and ideas), whether in written or oral form (hereinafter also referred to as the "Information"). All Information is of a confidential nature and is received for the sole purpose of performance under the Agreement.

13.2. Information shall be kept confidential and shall not be used for any different or further purpose other than the purposes set forth in the Agreement. Each party agrees that Information received from the other party will be transmitted, to the extent strictly necessary, only to those directors, employees, consultants, and subcontractors who: (i) have a need to know the same for the purposes set forth in the Agreement; (ii) are informed of the confidential nature of the Information; and (iii) agree to comply with the provisions of the Agreement and to use the Information only for the purposes set forth in the Agreement.

13.3. Each party shall be jointly and severally liable with its directors, employees, consultants, and subcontractors who have violated the provisions of this article, without the benefit of the right of prior discussion, for any violation committed by them.

13.4. In the absence of the prior written consent of the other party, each party agrees not to disclose in whole or in part, including by indirect reference, the Information to third parties other than those entitled to access the same based on specific provisions of the Agreement, and not to disclose the existence or content of the Information and this Agreement.

13.5. Each party will protect the other party's Information from unauthorized disclosure, using at least the same degree of care used to protect and safeguard its own Information of a similar nature, and in each case using due caution to prevent unauthorized use and publication.

13.6. Each party shall not acquire any rights to the Information of the other party.

13.7. It is not to be considered a piece of Information all that is:

- 13.7.1. already in the public domain or already known to the receiving party.
- 13.7.2. published or put in the public domain, but not because of a breach of either party's confidentiality obligations.
- 13.7.3. disclosed by third parties, successors in title.
- 13.7.4. developed by the receiving party independently and without any connection to the transfer of Information for the purpose of service delivery.
- 13.7.5. necessarily disclosed in connection with steps each party should take to enforce in court its rights under the Contract, to the extent that the waiver of confidentiality obligations is necessary for the purposes of judicial protection.

13.8. In addition, each party may disclose Information of the other party if expressly required to do so by law or by public authorities in the exercise of its functions. In such a case, the party involved will promptly notify the other party and act to protect, to the greatest extent possible, the confidentiality of the Information.

13.9. Each party agrees to return or destroy the other party's Information at the end of the Contract and in any case, at any time, if the other party so requests, provided that this does not affect the performance of the Contract.

13.10. The confidentiality obligations under this article shall remain in effect until each piece of Information becomes public knowledge for reasons other than the receiving Party's failure to fulfill its obligations under this clause.

## 14. Express termination clause – termination

14.1. Without prejudice to further provisions of this Agreement, given the nature, subject matter and limitation of the right of use covered by this License, Pikered shall have the right to terminate the Agreement by simple written notice from Pikered to the Customer pursuant to Article 1456 of the Italian Civil Code, without prejudice to compensation for damages, in the event of breach of one or more of the following obligations:

- 14.1.1. Clauses 5.1, 5.2, 5.3 regarding Pikered's intellectual property rights on the software and limitations on its use.
- 14.1.2. Clause 10.2 regarding the acquisition of permits for extra-EU export.
- 14.1.3. Clause 133 regarding confidentiality obligations.

14.2. Without prejudice to any further provisions of this Agreement and without prejudice in any case to compensation for damages, in the event of Customer's failure to comply with any other obligation set forth in this Agreement, which is not remedied within 15 days from Pikered's written warning, this Agreement shall be automatically terminated upon the expiration of the said period pursuant to Article 1454 of the Italian Civil Code.

14.3. Termination shall result in the interruption of the Software provision and withdrawal of the License and the amount already paid as consideration shall in no way be refunded or recalculated based on the period of use.

## 15. Force Majeure

15.1. Pikered shall not be liable for any alleged or actual damage or loss resulting from force majeure and/or total or partial non-performance or inaccurate performance due to the actions of military or civil authorities, governmental measures, earthquakes, fires, floods, epidemics, pandemics, quarantines, energy crises, strikes, wars, riots, terrorism, accidents, lack of resources, transportation delays, or any other cause beyond its reasonable control. Pikered will resume the performance of its obligations as soon as reasonably possible.

## 16. General Provisions

16.1. This Contract reflects the entire existing agreement between the Customer and Pikered. If any provision of this Contract is held invalid or ineffective, any such invalidity or ineffectiveness shall not affect the remaining provisions of the Contract. Pikered can assign or transfer all or part of its obligations under this Agreement or entrust the execution to qualified third parties or affiliated and/or subsidiary companies.

## 17. Applicable Law

17.1. This Contract shall be governed by Italian law. The provisions of the United Nations Convention on Contracts for the International Sale of Goods shall not apply.

## 18. Place of Jurisdiction

18.1. Any dispute, controversy or legal matter arising out of or relating to this Agreement, its conclusion, performance, default, termination, validity, invalidity, inexistence, use of the Software and any alleged consequential or related damages shall be subject to the exclusive jurisdiction of the Italian courts and the exclusive place of jurisdiction will be that of Milan, Italy, with the exclusion of all other jurisdictions.

# Annex A

## Data Processing Agreement

## art.28 EU Regulation 2016/679 (GDPR)

This agreement is an annex to the contractual agreement between Pikered S.r.l. ('Provider') and a party which, plays the role of Data Controller or Data Processor, according to the definitions provided for the two cases in Article 4 no. 7 and 8 of the EU Regulation 2016/679. These entities are jointly identified as Parties to this Agreement.

WHEREAS that:

- the Data Controller, according to the provisions of the law, is responsible for all processing decisions;

- Article 4 paragraph 1 no. 8 of the EU Regulation 2016/679 (hereinafter referred to as the 'Regulation') defines the Data Processor as 'the natural or legal person (...) who processes personal data on behalf of the Data Controller';

- pursuant to Art. 28 of the EU Regulation 2016/679, the Data Controller may entrust the performance of a single or a plurality of processing operations to another entity for this purpose, designating it as 'Data Processor';

- pursuant to Art. 28 para. 1 of the EU Regulation 2016/679, the Data Controller may only have recourse to data processors who, by virtue of their experience, capacity and reliability, offer sufficient guarantees to implement appropriate technical and organisational measures so that the processing meets the requirements of the EU Regulation 2016/679 itself and ensure the protection of the rights of the Data Subject

- the parties have in place a contract(s), or other legal act(s) (hereinafter the 'Contract'), of which this Agreement is an annex governing the arrangements with respect to the processing of personal data, which involves/concurs from the Provider in its role as Data Processor or Sub-Processor

- within the framework of the performance of the Agreement, the supplier in its role of Data Processor or Sub-Processor, implements - with a certain degree of autonomy in the choice of instruments - personal data processing operations (as defined by current legislation), on behalf of the Controller, who takes the decision(s) as to the purposes, methods and means of the processing;

- the Controller is also legally obliged and required to provide the supplier in its role as Data Processor or Sub-Processor with binding instructions/directives on certain legal and operational aspects of the processing itself and to ensure that the supplier's actions in its role as Data Processor or Sub-Processor comply with such directives

- it is the intention of the Data Controller to allow the supplier in his role as Data Processor or Sub- Data Processor, to the subjects within his company organisation who have been expressly authorised, access to the personal data whose knowledge is necessary to fulfil the Contract;

Having acknowledged the foregoing, the Data Controller (or the Data Processor in the event the supplier acts in the role of Sub-Processor) hereby

## APPOINTS

The supplier, as identified above, as Data Processor or Sub-Processor for the processing of the personal data necessary for the performance of the service entrusted under the aforesaid Contract, in compliance with EU Regulation 2016/679, Legislative Decree No. 196/2003 and ss.mm.ii., as well as with the guidelines issued and to be issued by the Supervisory Authority and by the European Data Protection Board. The Processing of Personal Data shall be limited to the purpose of the proper performance of all the service activities better provided for in the Contract mentioned in the introduction and the fulfilment of the relevant contractual and legal obligations.

The Data Controller declares that the data it transmits to the supplier in its role of Data Processor or Sub-Processor, are collected and transmitted in compliance with the regulations in force, are accurate and, if necessary, updated, are pertinent, complete and not excessive in relation to the contractual and pre-contractual purposes for which they are transmitted.

It is agreed between the parties that the supplier in his role as Data Processor or Sub-Processor and his sub-processors are obliged to process personal data in compliance with the principles and provisions of the EU Regulation 2016/679 and in general with the legislation on the protection of personal data of the measures of the competent Supervisory Authority, and, in any case, following the written instructions of the Data Controller.

It is agreed between the parties that the terms and conditions set out in the section entitled 'Appendix 1 - *Description of the processing activities*' at the end of this document form an integral and substantive part of this agreement.

This agreement governs the rights and obligations of the supplier in its role as Data Processor or Sub-Processor when the latter is processing personal data on behalf of the Data Controller.

This Agreement does not exempt the Provider in its role as a Data Processor or Sub-Processor from its obligations under the EU Regulation 2016/679 - General Data Protection Regulation or other legislation relating to the protection of personal data.

## 1. Object

The purpose of this agreement is to define the modalities by which the supplier in its role as Processor or Sub-Processor undertakes to carry out, on behalf of the Controller, the personal data processing operations defined below.

The supplier in its role as Data Processor or Sub-Processor undertakes to put in place appropriate technical and organisational measures so that the data processing carried out on behalf of the Controller meets the requirements of EU Regulation 2016/679 and ensures the protection of the rights of Data Subjects.

In fulfilment of its obligations under the Contract and this Deed, the Provider in its role as Data Processor or Sub-Processor shall therefore:

- comply with all the rules on the protection of personal data applicable to the processing, in particular with the provisions set forth in EU Regulation 2016/679 by Legislative Decree 196/2003 and subsequent amendments and additions, as well as comply with the guidelines issued and enacted by the Italian Data Protection Authority and the European Data Protection Board;

- process, in compliance with the instructions given for this purpose by the Controller and, in any case, in a manner compatible with the purposes for which the data were collected and communicated, only the personal data forming the subject matter of the Contract

- inform the Data Controller in advance in the event that the law applicable to the supplier in his role as Data Processor or Sub-Processor allows the latter to process the data in a manner contrary to the instructions given to him, in order to allow the Data Controller to exercise his right to object to the processing.

## 2. Description of the services of the Data Processor/Sub-Processor

The supplier in his role as Data Processor or Sub-Processor is authorised to process on behalf of the Controller the personal data necessary for the performance of the Contract.

The operations on personal data to be performed by the supplier in his role as Data Processor or Sub-Processor on behalf of the Controller are contractual in nature.

The purposes of the processing of data, as defined by the Controller, are attributable to the performance, by the supplier in his role as Data Processor or Sub- Data Processor, of all the services connected with the Contract referred to in the introduction.

For the performance of the service covered by the Contract, the Data Controller shall make available to the supplier in its role as Processor or Sub-Processor the details contained in 'Appendix 1 - *Description of Processing Activities*'. This appendix represents the definition of the processing activities to be performed by the supplier in its role as Processor or Sub-Processor on behalf of the Controller. The contents of the aforementioned appendix may change over time in accordance with new processing requirements of the Controller that may be regulated by amending and/or supplementing the Contract.

## 3. Duration of appointment and data processing

The subject matter of this writing shall take effect from the date of signing of this document and, in any event, with the commencement of any processing of personal data carried out on behalf of the Controller. This agreement shall remain in force until the expiry of the Contract cited in the foreword, or until such earlier termination as the Controller and/or Processor may exercise for any reason whatsoever.

The termination of the Contract cited in the foreword or the early revocation of the appointment shall entail the immediate cessation of processing and the completion of the activities specifically envisaged in the following article 'Disposal of data upon termination of contractual services'.

In any case, the supplier, in his role as Data Processor or Sub-Processor, remains obliged to maintain absolute confidentiality with regard to the data processed as governed by Article 5 below.

## 4. Obligations of the supplier in its role as data processor or sub-processor vis-à-vis the data controller

The supplier in its role as Data Processor or Sub-Processor undertakes to:

1. Only process data for the purpose(s) specified above and for the performance of contractual services.

2. The supplier in its role as Controller or Sub-Processor shall only process personal data upon the documented instructions of the Controller and/or the Processor, except where required by Union law or by the national law of the member state to which the supplier in its role as Controller or Sub-Processor is subject. The Controller and/or the Processor may issue subsequent instructions during the period of processing of personal data, but these must always be documented and kept in writing, including electronically.

3. If the Provider in its role as Data Controller or Sub-Processor considers that an instruction constitutes a violation of the EU Regulation 2016/679 or other provisions of Union or member state law, relating to the protection of personal data, it must immediately inform the Controller and/or the Processor.

4. Ensure the confidentiality of personal data processed under this Agreement.

5. The supplier in its role as controller or sub-processor shall only grant access to personal data processed on behalf of the controller to persons under its authority who have committed themselves to confidentiality or have an appropriate legal obligation of confidentiality and only in cases of actual necessity. The list of persons granted access must be reviewed periodically. On the basis of this review, access to personal data may be withdrawn if it is no longer necessary and, consequently, personal data shall no longer be accessible to these persons.

6. Check that persons authorised to process personal data under this Act:

a. undertake to observe confidentiality or are subject to an appropriate legal obligation of secrecy

b. receive the necessary training and instructions on the protection of personal data.

7. The supplier in its role as Processor or Sub-Processor shall, at the request of the Controller and/or Processor, demonstrate that authorised persons under its authority are subject to the aforementioned confidentiality.

8. Respect, in the choice of products, applications and/or services used for the processing entrusted to him/her, the principle of data protection by design (Privacy by Design) and of protection by default (Privacy by Default), as prescribed by Article 25 of EU Regulation 2016/679.

9. The supplier in his role as Data Processor or Sub-Processor also reserves the right to process data anonymously for the pursuit of any further purposes.

10. The supplier undertakes to notify the Data Controller or Data Processor, if acting as Sub-Processor, of any request received from the Data Protection Authority, the Judicial Authority or other Public Authority, within 1 day of receipt of the request, unless such notification is precluded by applicable legislation. The supplier shall, to the extent of its competence, provide the Data Controller with the necessary support to respond to the above requests.

## 5. Transfer of data to third countries or international organisations

Any transfers of personal data to third countries or international organisations shall only take place on the basis of documented instructions from the Data Controller and shall always take place in accordance with Chapter V of EU Regulation 2016/679.

Where transfers of data to third countries or international organisations, for which the Data Controller has not provided instructions, are required by EU or Member State law to which the Provider is subject in its role as Data Controller or Sub-Processor, the Provider shall

inform the Data Controller of this legal obligation prior to processing, unless EU or Member State law prohibits such information for important public interest reasons.

Within the framework of this Agreement, the Provider in its role as Data Controller or Sub-Processor, if it does not have documented instructions from the Data Controller, may therefore not:

1. transfer personal data to a Data Controller or a Processor or a Sub-Processor in a third country or international organisation;

2. transfer the processing of personal data to a Controller or Sub-Processor in a third country;

3. have the personal data processed by Processors or Sub-Processors in a third country.

The transfer, even temporarily, outside the territory of the European Union, by any form or means, of personal data processed in the performance of the Contract, may be allowed to the supplier in its role as Data Processor or Sub-Processor, where strictly necessary, only where it is done in compliance with the provisions of Articles 44 et seq. of EU Regulation 2016/679. Apart from the above cases, the transfer, even temporarily, by any form or means, of processed personal data to a country outside the European Union is prohibited when the law of the country of destination or transit of the data does not ensure an adequate level of data protection.

## 6. Duty of confidentiality of the Data Processor/Sub-Data Processor and persons acting on his behalf

In connection with the subject matter of the Agreement and this deed, the parties have exchanged and will continue to exchange information concerning the personal data of the data subjects. All such information shall be deemed confidential.

The Supplier in its role as Data Controller or Sub-Processor undertakes to adopt all necessary and useful measures so as not to prejudice the confidentiality of the information and to ensure that its employees and anyone else assigned to process the personal data provided by the Data Controller and/or the Processor and in general processed on behalf of the Data Controller comply with the provisions of the applicable data protection legislation, as well as with the instructions set forth in this deed and any other written instructions that may be communicated to it by the Data Controller.

The confidentiality undertakings provided for herein shall remain valid and effective even after the expiration of the Contract or the early termination of the appointment, the supplier in his role as Data Controller or Sub Data Controller shall ensure that the persons who are granted access to the confidential information are subject to legal or contractual confidentiality obligations.

## 7. Additional Sub-Processors

In order to be able to engage another Sub-Processor, the supplier in its role as Processor or Sub-Processor must meet the requirements of Article 28(2) and (4) EU Regulation 2016/679.

The supplier in its role as Processor or Sub-Processor may not, therefore, engage another Sub-Processor for the performance of the Agreement and this Agreement without the prior written general authorisation of the Controller and/or the Processor.

The supplier in its role as Processor or Sub-Processor shall have the general authorisation of the Controller and/or the Processor for the purpose of entrusting further Sub-Processors. The supplier in its role as Processor or Sub-Processor shall inform the Controller and/or the Processor in writing of any changes in terms of addition or replacement of Sub-Processors, thereby ensuring that the Controller and/or the Processor has the opportunity to object to such changes prior to the assignment of the Sub-Processors. The updated Sub-Processor list can be found in the supplier's Web site: https://www.pikered.com/en/documents/.

When the supplier in its role as Processor or Sub-Processor employs an additional Sub-Processor to perform specific processing activities on behalf of the Controller and/or Processor, the following obligations are imposed on such additional Sub-Processor by means of a contract or other legal act under EU or Member State law, the same data protection obligations contained in this Agreement, providing in particular sufficient safeguards to put in place appropriate technical and organisational measures so that the processing meets the requirements of this Agreement and EU Regulation 2016/679.

It is therefore incumbent on the supplier in its role as Processor or Sub-Processor to require that the additional Sub-Processor fulfils at least the obligations to which it is subject under this Agreement and EU Regulation 2016/679.

The provider in its role as Processor or Sub-Processor agrees a third-party beneficiary clause with the additional Sub-Processor, whereby, in the event of the former's bankruptcy, the Controller and/or Processor is a third-party beneficiary of the agreement relating to the additional Sub-Processor and is entitled to enforce the agreement against that Sub-Processor, e.g. by allowing the Controller and/or Processor to require the additional Sub-Processor to erase or return personal data.

In the event that the additional Sub-Processor fails to fulfil its data protection obligations, the provider in its role as Controller or Sub-Processor retains towards the Controller and/or Processor the entire responsibility for the fulfilment of the obligations of such additional

Sub-Processor. This is without prejudice to the data subjects' rights under the EU Regulation 2016/679 (in particular those provided for in Articles 79 and 82 EU Regulation 2016/679) vis-à-vis the Data Controller and the Processor, including the Sub-Processor.

## 8. Systema administrator

If the nature of the task entrusted to the supplier in his role as Data Processor or Sub-Processor, the details of which are set out in the Contract between the parties, envisages the use of users with system administrator authorisation levels, the requirements set out in the general provision - 27 November 2008 'Measures and precautions prescribed for data controllers of processing operations carried out by electronic means with regard to the attribution of system administrator functions' (G. U. no. 300 of 24/12/2008 and subsequent amendments), issued by the Garante Garante di Tutela di Tutela. U. No. 300 of 24/12/2008) and subsequent amendments, issued by the Personal Data Protection Authority.

This provision requires the traceability and recording of system administrator access activities. These records (access logs) must have characteristics of completeness, inalterability and possibility of verifying their integrity that are adequate to achieve the purpose for which they are required. The records must include references to the 'username' used, time references and a description of the event (log in, attempted log in, log out) that generated them and must be kept for an appropriate period of time that must not be less than six months.

Pursuant to the provisions contained in the aforementioned Garante Order, the parties acknowledge that the Data Controller, the Data Processor and the Sub-Processor shall set up and manage systems suitable for recording logical accesses (computer authentication) to processing systems and electronic archives by all persons designated as system administrators, whether belonging to the organisation of the Data Controller and/or the Data Processor and/or the Sub-Processor.

Each person designated as system administrator, who shall be selected on the basis of a prior assessment of experience, capacity and reliability, as well as of the ability to provide an adequate guarantee of full compliance with the applicable processing provisions, including the security profile, shall be provided with a personal username, the credentials of which shall be the sole responsibility of the same.

The supplier in its role as Data Controller or Sub-Processor undertakes to maintain a register of the names of the persons designated as system administrators, as well as the personal credentials assigned to them.

The Data Controller and/or the Processor may carry out annual audits on the activities performed by the supplier in its role as Processor or Sub-Processor with regard to the personnel designated as System Administrator. It is the supplier's obligation in its role as Data Processor or Sub-Processor to provide the Data Controller and/or the Data Processor with full cooperation in the performance of such audits; in any event, the supplier is required to prepare periodic written reports, also in the form of intervention reports, of the activities performed in the performance of the tasks entrusted to it under this deed and the contract between the parties.

## 9. Right to information of data subjects

It is the responsibility of the data controller to provide the information referred to in Articles 13-14 to the data subjects for processing operations.

## 10. Exercise of data subjects' rights

As far as possible, the supplier in its role as Data Controller or Sub-Processor must assist the Data Controller and/or the Sub-Processor, in fulfilling its obligations, to follow up on requests to exercise the rights of data subjects provided for in Articles 15-22 of the EU Regulation 2016/679: right of access, rectification, erasure and objection, right to restriction of processing, right to data portability, right not to be subject to automated individual decision-making (including profiling).

If data subjects exercise their right by sending the request to the supplier in its role as Data Processor or Sub-Processor, the latter must forward it by e-mail to the addresses indicated in the Contract, no later than the fourth day immediately following receipt of the request.

The supplier in its role as Processor or Sub-Processor shall also, within 5 days of receipt of the request received by it, forward by e-mail to the addresses indicated in the Contract, all the information in its possession that is useful for responding to the Data Subject.

The supplier in its role of Data Processor or Sub-Processor is not obliged to reply directly to the Data Subject without the prior written authorisation of the Data Controller and/or Data Processor.

This is without prejudice to any different documented indications provided by the Controller and/or the Processor or to any legal requirement applicable to the provider in its role as Processor or Sub-Processor (who is obliged, to the extent required by law, to inform the Controller and/or the Processor of such legal requirement before the provider in its role as Processor or Sub-Processor responds to the Data Subject's request).

## 11. Personal data breach notification

The supplier in its role as Data Processor or Sub-Processor shall notify the Controller and/or the Processor of any personal data breach within a maximum period of 48 hours after becoming aware of it. Such notification shall be accompanied by any relevant documentation enabling the Controller, if necessary, to notify the breach to the competent supervisory authority.

It is up to the Data Controller alone to decide not to notify the competent supervisory authority in the event of a simple incident that did not result in the loss, destruction, dissemination or modification of the data and/or, despite the personal data breach, is unlikely to pose a risk to the rights and freedoms of the Data Subjects. The supplier in its role as Data Processor or Sub-Processor shall provide the Controller and/or the Processor with all information within its competence in order to allow the Controller to make such an assessment.

The notification must at least:

(a) describe the nature of the personal data breach including, where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of personal data records concerned;

(b) provide the name and contact details of the Data Protection Officer or other contact point from which more information may be obtained

(c) describe the likely consequences of the personal data breach

(d) describe the measures taken or proposed to be taken to remedy the personal data breach and also, where appropriate, to mitigate its possible adverse effects.

If and to the extent that it is not possible to provide the information at the same time, it may be provided at a later stage without further undue delay.

The supplier in its role as Data Controller or Sub-Processor shall make information available to the Data Controller / or the Data Processor to enable communication to the data subject in the event that the incident may involve a high risk.

This information should describe, in clear and simple terms, the nature of the personal data breach and contain at least

a. a description of the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned

b. the provision of the name and contact details of the Data Protection Officer or other contact point where more information can be obtained

c. a description of the likely consequences of the personal data breach

d. a description of the measures taken or proposed to be taken to remedy the personal data breach and also, where appropriate, to mitigate its possible adverse effects.

## 12. Assisting the supplier in its role as Data Controller or Sub-Processor in implementing the obligations of the Controller and/or the Processor

The provider in its role as Data Controller or Sub-Processor shall assist the Controller and/or the Processor in carrying out data protection impact assessments, in accordance with Article 35 of the EU Regulation 2016/679.

The provider in its role as Data Controller or Sub-Processor assists the Controller and/or the Processor in the prior consultation of the supervisory authority, provided for in Article 36 of the EU Regulation 2016/679.

## 13. Security measures

Article 32 of the EU Regulation 2016/679 provides that taking into account the state of the art and the cost of implementation, as well as the nature, subject matter, context and purposes of the processing, as well as the risk of varying degrees of likelihood and severity to the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

The controller must assess 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, measures may include the following:

a. the pseudonymisation and encryption of personal data;

b. the ability to ensure the confidentiality, integrity, availability and resilience of processing systems and services on an ongoing basis;

c. The ability to promptly restore the availability and access of per- sonal data in the event of a physical or technical incident;

d. a procedure to regularly test, verify and evaluate the effectiveness of technical and organisational measures to ensure the security of processing.

Pursuant to Article 32 EU Regulation 2016/679, the provider in its role as Data Controller or Sub-Processor shall also assess, independently of the Data Controller and/or Data Processor, the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this end, the Controller and/or Processor shall provide the provider in its role as Processor or Sub-Processor with all the information necessary to identify and assess such risks.

Furthermore, the supplier in its role as Data Controller or Sub-Processor shall assist the Data Controller and/or the Processor in ensuring compliance with the obligations imposed on the latter pursuant to Article 32 EU Regulation 2016/679 by, inter alia, providing it with information regarding the technical and organisational measures already implemented by the latter pursuant to said Article 32, together with all other information necessary for the Data Controller and/or the Processor to comply with the obligations imposed on the latter pursuant to said Article 32.

## 14. Disposal of data upon termination of contractual services

Upon termination of the provision of services relating to the processing of these data, the supplier in its role as Data Processor or Sub-Processor undertakes to:

- return all data of a personal nature to the Controller and/or Processor and/or

- transmit the personal data to the Data Controller and/or Sub-Processor designated by the Controller and/or Processor.

This operation must be accompanied by the destruction of all copies existing in the supplier's information systems in its role as Data Controller or Sub-Processor. The result of the destruction of the data must be documented and communicated in writing by the supplier in its role as Data Controller or Sub-Processor.

## 15. Data Protection Officer

The supplier in its role as Data Controller or Sub-Processor shall inform the Controller and/or the Processor of the name and contact details of its Data Protection Officer, if it has designated one in accordance with Article 37 of EU Regulation 2016/679.

## 16. Register of categories of processing activities

The provider in its role as Data Processor or Sub-Processor declares that it keeps the register of all categories of processing activities carried out on behalf of the Controller and/or the Processor, as required by Article 30(2) of EU Regulation 2016/679.

The register must contain:

- the name and contact details of the Data Controller on whose behalf he or she processes, of any Processors and, if applicable, of the Data Protection Officer;

- the categories of processing operations carried out on behalf of the Controller;

- where applicable, the transfers of personal data to a third country or to an international organisation and, in the case of transfers provided for in Article 49(1), second subparagraph, of the EU Regulation 2016/679, the documents certifying the existence of appropriate safeguards;

- as far as possible, a general description of the technical and organisational security measures, including, among others, as required:

- the pseudonymisation and numbering of personal data;

- the means to ensure the continued confidentiality, integrity, availability and resilience of processing systems and services;

- the means to re-establish the availability of and access to personal data at the appropriate times in the event of a physical or technical incident;

a procedure for regularly testing, analysing and evaluating the effectiveness of technical and organisational measures to ensure the security of processing.

## 17. Documentation

The supplier in its role as Processor or Sub-Processor shall make available to the Controller and/or Processor the documentation necessary to demonstrate compliance with all obligations and to allow audits and verifications, including inspections, to be carried out by the Controller and/or Processor or another auditor whom he has mandated, and contribute to these audits.

The Controller and/or the Processor shall ensure that:

(i) the audits, inspections and verifications referred to in the preceding paragraph will take place during normal working hours and without hindering the activity of the supplier in its role as a Data Processor or Sub- Data Processor and of other clients of the same supplier;

(ii) all information obtained or generated by the Data Processor and/or Sub-Data Processor or its auditor(s) in connection with such audits, inspections and reviews shall be kept strictly confidential (except as required by the Supervisory Authorities or, if otherwise required by applicable law).

The Controller and/or Processor acknowledges and agrees that the cost of such audits, checks or inspections shall be borne by the Controller and/or Processor, unless such audits, checks or inspections result in non-compliance and/or breach by the Provider in its role as Controller or Sub-Processor of its obligations.

As an alternative to the aforementioned inspections and checks, the Controller and/or the Processor may request from the supplier in its role as Processor or Sub-Processor the documents representing the results of the periodic checks and audits that the supplier in its role as Processor or Sub-Processor must implement pursuant to Article 32(1)(d) of EU Regulation 2016/679.

## 18. Obligations of the Controller and/or the Processor vis-à-vis the supplier in its role as Processor or Sub-Processor

The Data Controller shall be solely responsible for all assessments regarding the lawfulness of the processing and the safeguarding of the rights of the Data Subjects. The Data Controller is responsible for ensuring that the processing of personal data is carried out in accordance with the EU Regulation 2016/679 (Art. 24 EU Regulation 2016/679), the applicable data protection provisions of the EU or the Member States.

The Data Controller has the right and the obligation to make decisions on the purposes and means of the processing of personal data.

It is the responsibility of the Data Controller, inter alia, to ensure that the processing of personal data for which the supplier is entrusted in its role as Data Processor or Sub-Processor has a valid legal basis.

The Data Controller has therefore assured the supplier in its role as Data Processor or Sub-Processor that all legal requirements for the processing have been met:

- having previously provided the Data Subjects with the information required by Articles 13 and 14 of EU Regulation 2016/679;

- having ensured the existence of a legal basis legitimating the lawfulness of the processing, including the express consent of the Data Subject, where required by the applicable law;

- having carried out any other fulfilment required for the processing of personal data by the applicable law.

The Data Controller and/or the Data Processor undertakes to:

- provide the Sub-Processor with the data provided for in the Appendix to this deed;

- document in writing all instructions concerning the processing of data by the supplier in its role as Data Controller or Sub-Processor;

- supervise, in advance and during the duration of all processing, compliance with the obligations under EU Regulation 2016/679 by the supplier in its role as Data Controller or Sub-Processor;

- supervise the processing, including reviews and inspections of the provider in its role as a Processor or Sub-Processor.

## 19. Liability

The parties to this agreement shall hold each other harmless for any damages, including legal fees, that may arise from claims made against each other as a result of any unlawful or improper processing operations that are attributable to the act, conduct or omission of the other.

Pursuant to Article 82 paragraph 2 of the EU Regulation 2016/679, the supplier in his role as Data Processor or Sub-Processor shall only be liable for any damage caused to the Controller and/or the Data Processor and/or the third parties concerned, resulting from the processing activities performed by him, if he has not fulfilled the obligations arising from the data protection legislation specifically directed to the Data Processors or has acted in a manner that is inconsistent with or contrary to the provisions of this contract or the lawful instructions of the Data Controller.

## 20. Start and resolution

This Agreement shall be effective from the date of signature by both parties. The parties shall have the right to request the renegotiation of this Agreement should a change in the law or its inadequacy give rise to such renegotiation.

This Agreement is valid for the duration of the performance of the services relating to the processing of personal data arising from the Agreement. be terminated, unless the parties have agreed on other Clauses governing such performance.

By signing this document, the parties mutually acknowledge that they have previously discussed its contents, that they have received a copy of it and, consequently, that they consider it to be a binding part of the Contract.

*Appendix 1 - Description of processing Activities'.*

The following Appendix describes the activities to be carried out by the supplier in its role as Processor or Sub-Processor in order to fulfil the Contract, undertaking to ensure an appropriate level of security. Where the supplier in his role as Processor or Sub-Processor has been authorised to appoint additional Sub-Processors, he shall ensure the same level of security as is required for the processing activities described in this Appendix.

Below are descriptions of the processing activities, broken down by software product purchased by the data controller:

| Object | Processing | Categories of data subjects | Types of personal data | Categories of personal data | Special categories of personal data (art. 9 of GDPR) |
|---|---|---|---|---|---|
| Execution of the software in the target infrastructure, as defined in the contract for the 'ZAIUX Evo' product (software in Cloud mode) | Listed below are the activities that may be performed during the execution of the contract:<br><br>o Access to the logs generated by the platform, for debugging purposes: they will not contain any information in addition to what is set out in this table, they may contain useful information in order to understand which 'attack' techniques are attempted by the software during execution<br><br>o Access to generated reports, for internal debugging purposes or following an explicit request by the Data Controller, to clarify their interpretation or report anomalies<br><br>o Access to and manipulation of BAS sandboxes during execution, for advanced debugging purposes or to correct anomalies during execution (by way of example and not limited to: disabling a technique that creates anomalies during the overall execution of the BAS due to a particular network configuration; in these cases, data such as plaintext passwords may be visible, this potential condition is the purpose of carrying out activities aimed at verifying the existence of vulnerabilities such as the possibility of accessing information in plain text that may entail a risk)<br><br>o Creation of logs to trace administrative actions of users inside the platform, | Natural persons to whom the personal data in the IT infrastructure subject to the execution of the software refer;<br><br>Users of the software | Common data<br><br>Any data belonging to special categories and/or judicial data present in the IT infrastructure subject to the execution of the software (such data are not the specific purpose of the processing) | Identification data<br><br>Authentication data<br><br>Role data | |

| | | | | | |
|---|---|---|---|---|---|
| | with a retention period of 12 months<br><br>The processing operations may be the following<br><br>collection, recording, organisation, structuring, storage, adaptation or modification, extraction, consultation, use, communication by transmission, comparison or interconnection, restriction, deletion or destruction; | | | | |
| Execution of the software in the target infrastructure, as defined in the contract for the 'ZAIUX Framework' product (software in on-premise mode) | The activities that may be performed in the execution of the contract are listed below:<br><br>o - Access to the software during execution in the target infrastructure, after the creation of a communication channel by our client (ZAIUX Framework is on-premise), with visibility of the techniques executed and, potentially, execution of attacks under the supervision of the Data Controller itself (with the purpose of supporting the client in the search for vulnerabilities)<br><br>o - Receiving and analysing any information sent by the Data Controller (by way of example but not limited to: output lists of attack techniques) useful for debugging purposes or the development of ad hoc attack modules to deal with particular situations.<br><br>The processing operations may be the following<br><br>collection, recording, organisation, structuring, storage, adaptation or modification, extraction, consultation, use, communication by transmission, comparison or interconnection, restriction, deletion or destruction; | Natural persons to whom the personal data in the IT infrastructure subject to the execution of the software refer | Common data<br><br>Any data belonging to special categories and/or judicial data present in the IT infrastructure subject to the execution of the software (such data are not the specific purpose of the processing) | Identification data<br><br>Authentication data<br><br>Role data | |