ANNEX I

DATA PROCESSING AND SECURITY AGREEMENT ("DPSA")

in accordance with art. 28 and 32 of EU Regulation no. 679/2016 ("GDPR")

This Data Processing and Security Agreement (hereinafter, "**DPSA**") must be attached to and forms an integral and substantial part of the Agreement executed between Cleafy and the Customer. All capitalized terms not defined in this DPSA have the meaning given to them in the Agreement.

Whether the Customer is located outside the EU and is not subject to the GDPR (with no obligation to appoint Cleafy as its data processor under art. 28 GDPR), only section 5 ("*Security Measures*") of this DPA and any clause referred therein apply between the parties.

If, at the contrary, the Customer is required to appoint a data processor under an applicable law of its jurisdiction in writing, this DPSA shall prevail over any other possible appointment drafted and submitted by the Customer to Cleafy.

It is in any event understood that, in relation to the processing of personal data carried out by Cleafy on behalf of Customers located outside the EU and not subject to the application of the GDPR, Cleafy undertakes to comply only with its obligations under the GDPR.

WHEREAS

(A) Under the Agreement, Cleafy shall provide to the Customer - inter alia - the Subscription Service, the Sandbox, the Professional Services and the CSS (hereinafter, for the sole purpose of this DPA, jointly referred to as "**Service/s**");

(B) for the purpose of providing these Services, Cleafy will necessarily process personal data on behalf of the Customer ("**Customer Data**" as defined in the Agreement) and in relation to such processing Cleafy will act as data processor (also, "**Data Processor**") and the Customer as data controller (also, "**Data Controller**");

(C) Customer declares to have verified that Cleafy provides sufficient guarantees to implement adequate technical and organizational measures aimed at ensuring that the aforesaid data processing of Customer Data is carried out in compliance with the principles and obligations set forth by GDPR – including the security measures and the compliance of any possible transfer of personal data outside the European Economic Area ("**EEA**") with the Commission Implementing Decision 2021/914 of 4 June 2021 on Standard Contractual Clauses ("**SCCs**")[1] - and that the protection of the rights of the data subjects is guaranteed.

ALL THIS BEING SAID

pursuant to the art. 28 and 32 of GDPR, the Parties intend to regulate the processing of the Customer Data referred to in art. 3 below carried out by Cleafy in its capacity as Data Processor.

1. PREMISES

1.1 The premises shall form an integral and substantial part of this DPSA.

2. SUBJECT-MATTER

2.1 By signing this DPSA, the Parties intend to regulate the conditions to which the Data Processor must adhere for the execution of the operations of processing of Customer Data referred to in art. 3 below.

2.2 The Data Processor informs the Data Controller to have designated and appointed a Data Protection Officer ("**DPO**") who can be contacted at the following e-mail address: dpo@cleafy.com.

2.3 Details of the processing operations, in particular the categories of Customer Data and the purposes for which such data are processed on behalf of the Data Controller, are specified in art. 3 below.

3. NATURE AND PURPOSE OF THE PROCESSING

3.1 The processing of Customer Data carried out by the Data Processor shall consist in carrying out the operations necessary to correctly provide the Services in favor of the Data Controller as well as to fulfill its obligations under the Agreement.

3.2 Such processing shall be carried out by the Data Processor in a lawful manner, according to correctness, in compliance with the principles set forth in art. 5 of GDPR, professional and business secrecy and in accordance with the instructions provided for by this DPSA and those that the Data Controller may give, from time to time, to the Data Processor.

[1] Standard Contractual Clauses (SCCs) are clauses for data transfers between EU and non-EU countries. According to the GDPR, contractual clauses ensuring appropriate data protection safeguards can be used as a ground for data transfers from the EU to third countries. This includes model contract clauses – so-called standard contractual clauses (SCCs) – that have been "pre-approved" by the European Commission. For further details on SCCs please visit this link: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

Specifically, the type of Customer Data that the Data Processor may process refer - but is not limited - generally to the following:

(i) personal user identifier data - they depend on user identification method chosen by the Data Controller, typically one or more User ID, e-mail address, name and surname, fiscal code, phone number, etc.;

(ii) payments data as bank account, payee, payment description, generally made by the Data Controller's clients;

(iii) technical data as browser or device fingerprint and IP Address.

4. OBLIGATIONS OF THE DATA PROCESSOR

4.1 In general, the Data Processor is required to:

i. process the Customer Data for the sole purpose of correctly providing the Services in favor of the Data Controller;

ii. process the Customer Data in compliance with the instructions given by the Data Controller with this DPSA and/or subsequently and, in any case, to operate in accordance with the provisions of GDPR and the applicable provisions of the Italian Data Protection Authority ("**Italian DPA**"). Any possible further instruction not listed in this DPSA that the Data Controller intends to provide to the Data Processor must be previously confirmed in writing by Data Processor.

Where Data Processor believes compliance with Data Controller's instructions could result in a violation of the GDPR and/or any other applicable data protection law or is not in the ordinary course of Data Processor's obligations in providing the Services, Data Processor shall promptly notify Data Controller thereof. No damages and/or lack of service and/or prejudice will be reimbursed by the Data Processor to the Data Controller due to the Data Processor's failure to perform processing operations under this DPSA as a result of any refusal of the Data Processor to comply with an unlawful instruction received by the Data Controller;

iii. make available to the Data Controller all the information necessary to demonstrate compliance with the obligations set forth in this DPSA and to allow and contribute to the audit activities, including inspections, carried out by the Data Controller or another authorized person, as indicated in art. 11 below;

iv. not communicate and/or disseminate the processed data to third parties, unless strictly necessary for the purposes of the processing and/or with the prior authorization of the Data Controller;

v. comply with the conditions and procedures set forth in art. 9 below for the appointment of any sub-processor;

vi. carry out, for the purposes of the correct application of the GDPR and the instructions provided by the Data Controller, periodic checks on the fulfilments and activities carried out by the subjects authorized to the processing and by their sub-processors;

vii. assist the Data Controller in the preparation of a possible data protection impact assessment ("**DPIA**") and in any prior consultation of the Italian Data Protection Authority, where deemed necessary, pursuant to art. 36 of the GDPR.

5. SECURITY MEASURES

5.1 The Data Processor guarantees that it has adopted the technical and organizational measures listed in the table below to meet the requirements of the GDPR and to protect the rights of the data subjects. The Data Processor assures that the processing operations will be carried out in compliance with the aforementioned security measures.

5.2 The Data Controller declares to have verified the security measures adopted by the Data Processor and that the same comply with art. 32 of the GDPR and ensure a level of security adequate to the risk that the processing of personal data may entail for the data subjects.

5.3 The Data Processor also undertakes to check and document, at least once a year, the state of implementation and/or updating of the aforesaid security measures, in order to avoid any breach of personal data (e.g., destruction, loss, alteration, unauthorized disclosure or access, etc.) or other unlawful form of processing, as well as to ensure respect of the confidentiality, integrity and availability of the Customer Data and their use exclusively for the purposes set out in art. 3 above.

A. **DATA SECURITY**	**SECURITY PROGRAM**	**ISO** Cleafy is ISO/IEC 27001, 27017 and 27018 certified. While providing the Subscription Service, Cleafy will maintain a written information security program of policies, procedures and controls aligned to ISO/IEC 27002, or substantially equivalent standard, governing the processing, storage, transmission, and security of Customer Data (the "Security Program"). The Security Program includes industry-standard practices designed to protect Customer Data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. Cleafy updates the Security Program to address new and evolving security technologies, changes to industry-standard practices, and changing security threats, although no such update will materially reduce the commitments, protections or overall level of service provided to Customer as described herein.
		SECURITY ORGANIZATION Cleafy shall designate a Chief Information Security Officer or an Information Security Manager responsible for coordinating, managing, and monitoring Cleafy's information security function, policies, and procedures.
		POLICIES Cleafy's information security policies shall be (i) documented; (ii) reviewed and approved by management, including after material changes to the Subscription Service; and (iii) published, and communicated to personnel, contractors, and third parties with access to Customer Data, including appropriate ramifications for non-compliance
		RISK MANAGEMENT Cleafy shall perform information security risk assessments as part of a risk governance program that is established with the objective to regularly test, assess and evaluate the effectiveness of the Security Program. Such assessment shall be designed to recognize and assess the impact of risks and implement identified risk reduction or mitigation strategies to address new and evolving security technologies, changes to industry standard practices, and changing security threats. Cleafy shall have the risk program audited annually by an independent third- party in accordance with Section 9.2 (Certifications and Attestations).
	PHYSICAL SECURITY MEASURES	Physical security measures are fully managed by a third party (Google LLC) which ensures the adoption of (1) physical access restrictions and monitoring that shall include a combination of any of the following: multi-zone security, man-traps, appropriate perimeter deterrents (e.g. fencing, berms, guarded gates), on-site guards, biometric controls, CCTV, and secure cages; and (2) fire detection and fire suppression systems both localized and throughout the data center floor. For a complete detail of the physical security datacenters measures refer to section "Appendix 2: Security Measures" of the Data Processing and Security Terms document publicly available on the Google GCP website (https://cloud.google.com/terms/data-processing-terms).
	TECHNICAL SECURITY MEASURES	**ACCESS ADMINISTRATION** Cleafy shall authorize its employees, contractors, and Subprocessors to access Customer instances only as strictly necessary to perform support and maintenance activities. Access to the Subscription Service by Cleafy employees and contractors is protected by authentication and authorization mechanisms. User authentication is required to gain access to production and sub-production instances. Individuals are assigned a unique user account. Individual user accounts shall not be shared. Access privileges are based on job requirements using the principle of least privilege access and are revoked upon termination of employment or consulting relationships. Access entitlements are reviewed by management

		quarterly. Infrastructure access includes appropriate user account and authentication controls, which will include the required use of VPN connections or similar/more advanced technology, complex passwords with expiration dates, account lock-out enabled, and a two-factor authenticated connection.
		SERVICE ACCESS CONTROL The Subscription Service provides user and role-based access controls. Customer is responsible for configuring such access controls within its instance.
		LOGGING AND MONITORING The production infrastructure log activities are centrally collected, are secured in an effort to prevent tampering and are monitored for anomalies by a Cleafy trained security team. Customer has full access to application audit logs within its instance(s), including successful and failed access attempts to Customer's instance(s). Audit logs are stored on the Subscription Service for 90 days or until the termination of the Subscription Service or the Evaluation Period. If the Customer needs a longer retention of such audit logs, API are available to programmatically access to the logs.
		FIREWALL SYSTEM An industry-standard firewall is installed and managed to protect the Customer production and sub-production instances by residing on the network to inspect all ingress connections routed to the Cleafy environment. Firewall rules comply with the whitelisting approach by restricting access only to sources authorized by the Customer. Customer shall be responsible for providing sources allowed to access to its instance(s). Rules are reviewed quarterly by Cleafy.
		VULNERABILITY MANAGEMENT Cleafy conducts yearly security risk evaluations to identify critical information assets, assess threats to such assets, determine potential vulnerabilities, and provide for remediation. When software vulnerabilities are revealed and addressed by a vendor patch, Cleafy will obtain the patch from the applicable vendor and apply it within an appropriate time frame in accordance with Cleafy's then-current vulnerability management and security patch management standard operating procedure and only after such patch is tested and determined to be safe for installation in all production systems.
		ANTIVIRUS Cleafy updates antivirus, anti-malware, and anti-spyware software on regular intervals and centrally logs events for effectiveness of such software.
		CHANGE CONTROL Cleafy evaluates changes to any technical component of the services to minimize risk and such changes are implemented following Cleafy's standard operating procedure.
		DATA SEPARATION Customer Data shall be maintained by Cleafy within a logical single-tenant architecture on multi-tenant cloud infrastructure that is logically and physically separate from Cleafy's corporate infrastructure. However, a restricted subset of fully-anonymized technical data shall be collected and processed by Cleafy on a multi-tenant platform in order to provide Cleafy Threat Intelligence.
		CONFIGURATION MANAGEMENT Cleafy shall implement and maintain standard hardened configurations for all system components within the Subscription Service. Cleafy shall use industry standard hardening guides, such as

		guides from the Center for Internet Security, when developing standard hardening configurations.
		DATA ENCRYPTION IN TRANSIT Cleafy shall use industry standard TLS 1.2 encryption to encrypt Customer Data in transit over public networks to the Subscription Service.
		DATA ENCRYPTION AT REST Cleafy shall provide encryption at rest capability with full-disk or server-side encryption for all the Services. This is done transparently without any changes to managed applications and without any actions on Customer parts required.
		SECURE SOFTWARE DEVELOPMENT Cleafy shall implement and maintain secure application development policies and procedures aligned with industry standard practices such as the OWASP Top Ten (or a substantially equivalent standard). All personnel responsible for secure application design and development will receive appropriate training regarding Cleafy's secure application development practices.
		SECURE CODE REVIEW Cleafy shall perform a combination of static and dynamic testing of code prior to the release of such code to Customers. Vulnerabilities shall be addressed in accordance with Cleafy software vulnerability management program. Software patches are regularly installed on Cleafy Cloud Customer instances.
		ILLICIT CODE The Subscription Service shall not contain viruses, malware, worms, date bombs, time bombs, shut-down devices, that may result in, either: (a) any inoperability of the Subscription Service; or (b) any interruption, interference with the operation of the Subscription Service (collectively, "Illicit Code"). If the Subscription Service is found to contain any Illicit Code that adversely affects the performance of the Subscription Service or causes a material security risk to Customer Data, Cleafy shall, as Customer's exclusive remedy, use commercially reasonable efforts to remove the Illicit Code or to advise and assist Customer to remove such Illicit Code.
	ORGANIZATIONAL SECURITY MEASURES	**PERSONNEL SECURITY** Cleafy performs background screening on all employees and all contractors who have access to Customer Data in accordance with Cleafy's then-current applicable standard operating procedure and subject to Law.
		PERSONNEL ACCESS MANAGEMENT Access to Personal Data by Data Processor will be limited to personnel who require such access to perform Data Processor's obligations under the Agreement and who are bound by obligations to maintain the confidentiality of such Personal Data at least as protective as those set forth herein and in the Agreement.
		SECURITY AWARENESS AND TRAINING Cleafy maintains a security and privacy awareness program that includes appropriate training and education of Cleafy personnel, including any contractors or third parties that may access Customer Data. Such training is conducted at time of hire and at least annually throughout employment at Cleafy.
		VENDOR RISK MANAGEMENT Cleafy maintains a vendor risk management program that assesses all vendors that access, store, process, or transmit Customer Data for appropriate security and privacy controls and business disciplines.

		SOFTWARE AND ASSET INVENTORY Cleafy shall maintain an inventory of all software components (including, but not limited to, Open-Source software) used in the Subscription Service, and inventory all media and equipment where Customer Data is stored.
		WORKSTATION SECURITY Cleafy shall implement and maintain security mechanisms on personnel workstations, including firewalls, anti-virus, and full disk encryption. Cleafy shall restrict personnel from disabling security mechanisms.
		MOBILE DEVICES SECURITY Cleafy shall implement and maintain security mechanisms on personnel mobile devices. Cleafy shall restrict personnel from disabling security mechanisms.
B. **SERVICE CONTINUITY**	**DATA MANAGEMENT & DATA BACKUP**	Cleafy will span the purchased instances of the Subscription Service in three different data centers (Zone) in the same region EU as defined in Google GCP documentations, backups are stored in a high-redundant copy in EU multi-regions bucket as defined in Google GCP documentations. Data centers attained SSAE 18 Type 2 attestations or have ISO/IEC 27001 certifications (or equivalent or successor attestations or certifications) acting in an active/active capacity for the Subscription Term). The purchased instance is fault-tolerant at a single component or an entire Zone failure. Data center provides redundancy at electrical, cooling and network level. The production database systems are spread in multiple copies in real-time across data centers in the same region. Each Customer instance is supported by a network configuration with multiple connections to the Internet. Cleafy backs up all Customer Data in accordance with Cleafy's standard operating procedure. This section does not apply to all Pre-GA Offerings, Sandbox and POC.
	DISASTER RECOVERY	Cleafy provides Recovery Point Objective (RPO) of 4 hours and a Recovery Time Objective (RTO) of 4 hours, and shall (i) maintain a disaster recovery ("DR") related plan that is consistent with industry standards for the Subscription Service; (ii) test the DR plan at least once every year on a customer-simulated environment; (iii) make available on Cleafy Customer portal (https://support.cleafy.com) summary test results which will include the actual recovery point and recovery times; and (iv) document any action plans within the summary test results to promptly address and resolve any deficiencies, concerns, or issues that prevented or may prevent the Subscription Service from being recovered in accordance with the DR plan. All Pre-GA Offerings, Sandbox (as defined in art. 12 of the Agreement) and POC do not meet such DR parameters, including RPO and RTO.
	BUSINESS CONTINUITY	Cleafy shall maintain a business continuity plan ("BCP") to minimize the impact to its provision and support of the Subscription Service from an event. The BCP shall: (i) include processes for protecting personnel and assets and restoring functionality in accordance with the time frames outlined therein; and (ii) be tested annually and updated based on any deficiencies identified during such tests.
	EXIT STRATEGY	The Cleafy Cloud services, according to a SaaS model, is not transferable in case of termination of the Agreement. However, due to the nature of the data managed by the services, it is unlikely the Customer will require a backup of the data. A set of Cleafy APIs are available, at no charge, to allow the Customer to export various subset of customer's data (refer to APIs documentation to get the full list of customer data available to be exported). The Customer may also request Cleafy's Professional Service to be supported in data exporting activities, it being understood that in

		such event the Customer shall pay Cleafy an extra fee for the provision of the above-mentioned Professional Service. This section does not apply to all Pre-GA Offerings, Sandbox and POC.
C. **MONITORING AND INCIDENT MANAGEMENT**	**INCIDENT MONITORING AND MANAGEMENT**	Cleafy will monitor, analyze, and respond to security incidents in a timely manner in accordance with Cleafy's standard operating procedure. Cleafy's security group will escalate and engage response teams as may be necessary to address a security incident. Through the Customer portal (https://support.cleafy.com) Customer could find the instructions to open an Incident ticket.
	BREACH NOTIFICATION	Cleafy will report without undue delay to Customer any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data (a "Breach") and in any case within the 24 hours.
	REPORT AND INCIDENT PROCESS	The goal of Processor's Incident response will be to restore the confidentiality, integrity, and availability of the Services environment and the Personal Data that may be contained therein, and to establish root causes and remediation steps. Depending on the nature and scope of the Incident, Processor may also involve and work with Controller and outside law enforcement to respond to the Incident. To the extent Processor becomes aware and determines that an Incident qualifies as a breach of security leading to the misappropriation or accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed on Processor systems or the services environment that compromises the security, confidentiality or integrity of such Personal Data ("Personal Data Breach"), Processor will inform Controller of such Personal Data Breach without undue delay. Processor will take reasonable measures designed to identify the root cause(s) of the Personal Data Breach, mitigate any possible adverse effects and prevent a recurrence. As information regarding the Personal Data Breach is collected or otherwise reasonably becomes available to Processor and to the extent permitted by law, Processor will provide Controller with (i) a description of the nature and reasonably anticipated consequences of the Personal Data Breach; (ii) the measures taken to mitigate any possible adverse effects and prevent a recurrence; (iii) where possible, the categories of Personal Data and Data Subjects including an approximate number of Personal Data records and Data Subjects that were the subject of the Personal Data Breach; and (iv) other information concerning the Personal Data Breach reasonably known or available to Controller or that Controller may be required to disclose to a public Authority or affected Data Subject(s). Unless otherwise required under Applicable Data Protection Law, the parties agree to coordinate in good faith on developing the content of any related public statements or any required notices for the affected Data Subjects and/or notices to the relevant public Authorities. The initial report will be made to Data Controller's security or privacy contact(s) designated in Cleafy's Customer Portal (or if no such contact(s) are designated, to the primary technical contact designated by Customer). As information is collected or otherwise becomes available, Data Processor shall provide without undue delay any further information regarding the nature and consequences of the Breach to allow Data Controller to notify relevant parties, including affected Data Subjects, government agencies and data protection authorities in accordance with Data Protection Laws. The report will include the name and contact information of the Data Processor contact from whom additional information may be obtained.
	DATA CONTROLLER OBLIGATIONS	Data Controller will cooperate with Data Processor in maintaining accurate contact information in the Customer portal (or other mechanism used to notify its customer base) and by providing any information that is reasonably requested to resolve any security

		incident, including any Breaches, identify its root cause(s) and prevent a recurrence. Data Controller is solely responsible for determining whether to notify the relevant supervisory or regulatory authorities and impacted Data Subjects and for providing such notice.
	COOKIES	When providing the Subscription Service, Cleafy uses cookies to: (a) track session state; (b) route a browser request to a specific node when multiple nodes are assigned; and (c) recognize a user upon returning to the Subscription Service. Customer shall be responsible for providing notice to, and collecting any necessary consents from, its users of the Subscription Service for Cleafy's use of cookies.
D. **PENETRATION TEST**	**BY A THIRD-PARTY**	Cleafy contracts with third-party providers to perform penetration tests on the Cleafy application to identify risks and remediations that help increase Cleafy's security posture. Cleafy shall make available executive reports from the penetration testing activities to Customer upon request.
	BY CUSTOMER	Customer could perform any security testing activities, including Penetration Testing, without Cleafy's prior authorization exclusively on the Sandbox provided by Cleafy. In any case, Customer shall not perform a penetration test without Cleafy's express written authorization on the Subscription Service. In the event Customer authorized penetration testing identifies vulnerabilities that Cleafy is able to reproduce, Cleafy shall, consistent with industry-standard practices, use commercially reasonable efforts to promptly make any necessary changes to improve the security of the services. Application stress tests performed by Customer, if intended as a part of acceptance testing and limited to the commissioning phase (i.e. before the application is released into production) are allowed. In such case, Customer shall notify Cleafy by submitting a request to schedule such a test using the Customer portal (https://support.cleafy.com) and shall sign Cleafy's application stress test agreement. Application stress tests are not authorized in any other production phase. Cleafy will perform in-house application stress tests on Customer-simulated environments in order to comply with the service level agreed in the CSA (Customer Support Addendum).

6. DURATION

6.1 This DPSA will enter into force on the date of the signature of the Agreement and will terminate on the end date or expiration of the Agreement. If such circumstances occur, the Data Processor undertakes to cease the processing of personal data immediately and to comply with the provisions of art. 7.

7. DELETION OF PERSONAL DATA

7.1 Where requested in writing by the Data Controller, Data Processor will delete Customer Data within the service in 10 (ten) business days. It remains in any case the Data Controller's right to ask for the return of Customer Data.

7.2 In any case, upon termination or expiration of the Agreement, all hosted and backed-up Customer Data will be securely removed within 30 (thirty) business days and cannot be recovered.

8. PROCESSING UNDER THE AUTHORITY OF THE DATA PROCESSOR

8.1 The Data Processor undertakes to identify its employees and/or any other natural persons (e.g., collaborators, consultants, etc.) who are authorized to process the Customer Data, giving them instructions and confidentiality obligations regarding the purposes, methods of processing, the nature of the data processed and security measures, in compliance with the provisions of the GDPR, applicable national legislation and this DPSA.

8.2 In this regard, the Data Processor hereby guarantees that the persons authorized to process the personal data will operate to protect the confidentiality of the data.

9. SUB-PROCESSORS

9.1 Data Controller confer to the Data Processors a general authorization to engage and appoint Sub-processors on the basis of a list previously agreed between the Parties (Annex III - Sub-processor Addendum). Any information about Sub-

processors, including their functions and locations, is available at the Data Processor's Customer Portal: https://support.cleafy.com (as may be updated by Cleafy from time to time in accordance with this DPSA).

9.2 In order to engage a Sub-Processor involved in any processing of Customer Data not previously listed in the Sub-Processor Addendum, Data Processor shall:

- notify Data Controller by e-mail or by notification within the Customer Portal (or other mechanism used to notify its customer base) the detail of Sub-processor ("**Data Processor's Notice**");
  and
- enter into a written agreement with such new Sub-processor requiring the Sub-processor abide by terms no less protective than those provided in this DPSA. The appointed Sub-processors shall be based in the European Economic Area ("EEA") or in a country non covered by an EU Commission's adequacy decision issued under art. 45 GDPR. In this cases, Data Processor will comply with the provisions of art. 12 of this DPSA for the transfer of personal data outside EEA.

9.3 It remains in any case understood between the Parties that the Data Controller shall only have the right to object to the addition, replacement or elimination by the Data Processor of one or more Sub-processors listed in Sub-processor Addendum and not to choose the Sub-processor to be engaged.

9.4 Upon written request by Data Controller, Data Processor shall provide to Data Controller a copy of the data processing agreement executed with the Sub-processors.

9.5 Data Controller may object to any modification of the Sub-processor Addendum by notifying Data Processor within 10 (ten) days after receipt of Data Processor's Notice, if Data Controller reasonably determines - based on grounded reasons – that such Sub-processor is and will be – after the assessment carried out in collaboration with the Data Processor - unable to process Customer Data in accordance with the terms of this DPSA ("**Objection Notice**"). If no notice is received by the Data Processor within the above deadline, the new Sub-processor shall be considered as approved by the Data Controller. In the event that Data Controller submits its Objection Notice, Data Processor shall reasonably consider such Objection and will notify Data Controller if it intends to provide the Services with the use of the Sub-processor at issue ("**Processor Notice**").

10. INDEMNITIES

10.1 The Data Controller hereby undertakes to indemnify and hold harmless the Data Processor from any liability and/or damage that may be recognized to the Data Processor as a result of the violation of any of the provisions of the GDPR, unlawfulness or incorrectness of the processing that is attributable to the fact, conduct or omission of the Data Controller and/or in any case attributable to the same and/or to persons authorized to process the personal data or who collaborate with it (such as, by way of example, employees, collaborators, consultants, etc.).

11. DATA CONTROLLER MONITORING RIGHTS

11.1 Data Processor shall provide Data Controller with reasonable assistance in relation to the security risk assessment which the latter may decide to perform with regard to the Services. It remains in any case understood that, with specific regard to the Customer Data owned and processed directly by the Data Controller, the Data Controller is solely responsible for determining the adequacy of the security measures adopted.

11.2 Cleafy shall establish and maintain sufficient controls to meet certification and attestation for the objectives stated in ISO/IEC 27001 and ISO/IEC 27018 (or equivalent standards) for the Security Program supporting the Services. At least every 3 (three) years, Cleafy shall obtain an assessment against such standards and audit methodologies by an independent third-party auditor and make the executive reports available to the Data Controller.

11.3 Data Processor shall allow for and contribute to audits that include inspections by granting Data Controller (either directly or through its representative(s), provided that such representative(s) shall enter into written obligations of confidentiality and non-disclosure directly with Cleafy) access to all reasonable and industry recognized documentation evidencing Cleafy's policies and procedures governing the security and privacy of Customer Data and its Security Program at no additional costs ("**Audit**") and provided that at least 10 (ten) calendar days prior notice is given by the Data Controller. The information available in Cleafy will include documentation evidencing Cleafy's Security Program, as well as Cleafy's privacy policies and procedures regarding personal information processed within the Services, copies of certifications and attestation reports (including audits) listed above.

11.4 Upon completion of the Audit, Data Processor and Data Controller may schedule a mutually convenient time to discuss the output of the Audit. Data Processor may, in its sole discretion, consistent with industry and Data Processor's standards and practices, make commercially reasonable efforts to implement Data Controller's suggested improvements noted in the Audit to improve Data Processor's Security Program, even charging to the Data Controller

more than the initially agreed upon price of Services if deemed necessary by the Data Processor. The Audit and the results derived therefrom are Confidential Information of Data Processor.

11.5 Any expenses incurred by the Data Controller in connection with or as a consequence of the Audit shall be borne exclusively by the Data Controller.

12. CUSTOMER DATA TRANSFERRED OUTSIDE EEA

12.1 The Data Processor undertakes to promptly inform the Data Controller if the regulations in force in the country to which the Data Processor belongs provide for the obligation to transfer the data outside the EEA, unless the notification of such communication is prohibited by the aforementioned regulations for important reasons of public interest.

12.2 In any event in which the Data Processor decides to engages Sub-processors - listed in the Sub-processor Addendum already approved by the Data Controller - which store, host and/or process Customer Data outside the EEA (in a country not subject to an adequacy decision by the EU Commission), the Data Processor grants to have executed with such Sub-processor the SCCs approved by the EU Commission and to provide the Data Controller with a copy of such SCCs where requested by the latter.

12.3 The Data Controller acknowledges that, according to Clause 2(a) of the SCCs, SCCs executed by a data processor with a data controller may contain other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, the SCCs or prejudice the fundamental rights or freedoms of data subjects. In this regard, the Data Processor declares to have checked the SCCs provided by the Sub-processors before signing them and that such SCCs contain the indication of certain security measures adopted by the Sub-processors that are similar and/or otherwise aligned with the Data Processors' security standards defined by this DPSA.

12.4 For the transfer of Customer Data outside the EEA (to a country not subject to an adequacy decision by the EU Commission), the Data Processor also declares to have carry out, before the transfer, a Transfer Impact Assessment ("TIA") in accordance with Clause 14 (a) - (d) of the SCCs and undertakes to provide the Data Controller with a copy of this TIA, where requested by the latter.

13. REQUESTS MADE FROM DATA SUBJECTS AND AUTHORITIES

13.1 During the validity of this DPSA, Data Processor shall provide Data Controller with the ability to access, correct, rectify, erase, or block Customer Data, or to transfer or port such data, within the Services, as may be required by the applicable laws (collectively, "**Data Subject Requests**").

13.2 Data Controller will be solely responsible for responding to any Data Subject Requests, provided that Data Processor shall reasonably cooperate with the Data Controller to respond to such Data Subject Requests to the extent that Data Controller is unable to fulfill such Data Subject Requests using the functionality in the Services. Data Processor will instruct the data subjects to contact the Data Controller in the event Data Processor receives a Data Subject Request directly.

13.3 In the case of a notice, audit, inquiry, or investigation by a government body, data protection authority, or law enforcement agency regarding the processing of Customer Data, Data Processor shall promptly notify the Data Controller unless prohibited by applicable law. Each party shall cooperate with the other party by providing all reasonable information requested in the event the other party is required to produce such information to a data protection authority.

14. APPLICABLE LAW AND JURISDICTION

14.1 This DPSA is governed by the provisions of the GDPR, as well as by national legislation on the protection of personal data of the countries to which the Data Controller and the Data Processor belong, unless they conflict with the provisions of the said GDPR. Disputes arising between the Data Controller and the Data Processor relating to this DPSA shall be submitted to the exclusive jurisdiction of the Court of Milan.

***