Data Processing and Security terms

Last modified: February 4, 2021

The customer agreeing to these terms ("Customer"), and Cleafy SpA or any other entity that directly or indirectly controls, is controlled by, or is under common control with Cleafy SpA (as applicable, "Cleafy"), have entered into an agreement under which Cleafy has agreed to provide Cleafy Cloud and related technical support to Customer (as amended from time to time, the "Agreement").

These Data Processing and Security Terms (the "Terms") will be effective and replace any previously applicable data processing and security terms as from the Terms Effective Date (as defined below). These Terms supplement the Agreement and they take precedence. Where the Agreement was entered into offline with Cleafy, these Terms supersede the "Privacy" Clause in that agreement (if applicable).

WHEREAS

(A) Customer acts as a Data Controller (the "Controller").

(B) Customer wishes to subcontract certain Services (as defined below), which imply the processing of personal data, to Cleafy SpA, acting as a Data Processor (the "Processor").

(C) The Parties seek to implement a data processing and security agreement that complies with the requirements of the current legal framework in relation to data processing and with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

(D) The Parties wish to lay down their rights and obligations.

IT IS AGREED AS FOLLOWS:

1. Definitions

1.1 "**Data Controller**" means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of Processing of Personal Data. For purposes of this DPA, Data Controller is Customer and, where applicable, its Affiliates either permitted by Customer to submit Personal Data to the Subscription Service or whose Personal Data is Processed in the Subscription Service.

1.2 "**Data Processor**" means the natural or legal person, public authority, agency, or other body which Processes Personal Data on behalf of the Data Controller. For purposes of this DPA, Data Processor is the Cleafy entity that is a party to the Agreement.

1.3 "**Data Protection Laws**" means all applicable laws and regulations regarding the Processing of Personal Data.

1.4 "**Data Subject**" means an identified or identifiable natural person.

1.5 "**Instructions**" means Data Controller's documented data Processing instructions issued to Data Processor in compliance with this DPA.

1.6 "**Personal Data**" means any information relating to a Data Subject uploaded by or for Customer or Customer's agents, employees, or contractors to the Subscription Service as Customer Data.

1.7 "**Process**" or "**Processing**" means any operation or set of operations which is performed upon Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure or

destruction.

1.8 “**Professional Services**” means any consulting or development services provided by or on behalf of Cleafy pursuant to an agreed statement of work or packaged professional services described or referenced in a signed ordering document.

1.9 “**Sub-Processor**” means any legal person or entity engaged in the Processing of Personal Data by Data Processor. For the avoidance of doubt, Cleafy’s colocation datacenter facilities are not Sub-Processors under this DPA.

1.10 “**Subscription Service**” means the Cleafy Cloud software as a service (SaaS) offering ordered by Customer under an Order Form, Use Authorization or other signed ordering document between Cleafy and Customer.

2. Duration

These Terms will, notwithstanding expiry of the Term, remain in effect until, and automatically expire upon, deletion of all Customer Data by Cleafy as described in these Terms.

3. Processing of Data

3.1 Instructions. The Agreement constitutes Data Controller’s initial written Instructions to Data Processor for Processing of Personal Data. Data Controller may issue additional or alternate Instructions provided that such Instructions are: (a) consistent with the purpose and the scope of the Agreement; and (b) confirmed in writing by Data Controller. For the avoidance of doubt, Data Controller shall not use additional or alternate Instructions to alter the scope of the Agreement. Data Controller is responsible for ensuring its Instructions to Data Processor comply with Data Protection Laws. Data Controller is solely responsible for assessing whether Data can be processed lawfully and for safeguarding the rights of Data Subjects. Data Processor will have no liability for any harm or damages resulting from Data Processor’s compliance with unlawful Instructions received from Data Controller. Where Data Processor believes compliance with Data Controller’s Instructions could result in a violation of Data Protection Laws or is not in the ordinary course of Data Processor’s obligations in operating the Subscription Service or delivering Professional Services, Data Processor shall promptly notify Data Controller thereof. Data Controller acknowledges Data Processor is reliant on Data Controller’s representations regarding the extent to which Data Controller is entitled to Process Personal Data.

3.2 Nature, Scope and Purpose of the Processing. Data Processor shall only Process Personal Data in accordance with Data Controller’s Instructions and to the extent necessary for providing the Subscription Service and the Professional Services, each as described in the Agreement. Data Controller acknowledges all Personal Data it instructs Data Processor to Process for the purpose of providing the Professional Services must be limited to the Customer Data Processed within the Subscription Service.

3.3 Categories of Personal Data and Categories of Data Subjects. Data Controller may submit Personal Data to the Subscription Service as Customer Data, the extent of which is determined and controlled by Data Controller in its sole discretion.

3.4. Data protection officer. The Processor provides assurance that it has engaged a competent and reliable data protection officer, who is granted the time required to perform his or her duties. The data protection officer performs the duties in accordance with the Legal Provisions; in particular, he/she takes steps to ensure compliance with the legal and agreed regulations regarding data protection. As far as the engagement of a data protection officer is not required by law and the Processor therefore does not have a data protection officer in place the Processor determines a contact person responsible for the matter of data protection.

4. Deletion or Return of Company Personal Data

4.1 Deletion or Return requested by Data Controller. Where requested, Data Processor will promptly and in any event within 15 business days supply a customer’s data in an industry standard format. Data

will be shared in ways that are convenient for the Data Processor. Where requested, Data Processor will promptly delete a customer's data within the service in 10 business days. Data will be automatically deleted from all other Data Processor systems within 180 days.

4.2 Deletion or Return on Termination. Upon contract termination or expiration of the Agreement, Data Controller has 30 days to request his data to be returned, after that time all hosted and backed-up data is automatically deleted and overwritten and cannot be recovered. Where requested, data will be provided in an industry standard format and will be shared in a way that is convenient for the Data Processor within 10 business days. After that time, all hosted and backed-up data will be securely removed within 10 business days and cannot be recovered.

5. Data Security

5.1 Security Program. While providing the Subscription Service, Cleafy will maintain a written information security program of policies, procedures and controls aligned to ISO27002, 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.

5.1.1 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.

5.1.2 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.

5.1.3 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).

5.2 Physical Security Measures. Physical security measures are fully managed by a third party (Google, Inc. (US)) 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 more information refer to section Appendix 2 (the "Security Measures") of the Data Processing and Security Terms document publicly available on the Google Cloud website.

5.3 Technical Security Measures.

5.3.1 Access Administration. 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, complex passwords with expiration dates, account lock-out enabled, and a two-factor

authenticated connection.

5.3.2 Service Access Control. The Subscription Service provides user and role-based access controls. Customer is responsible for configuring such access controls within its instance.

5.3.3 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 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).

5.3.4 Firewall System. An industry-standard firewall is installed and managed to protect Cleafy systems by residing on the network to inspect all ingress connections routed to the Cleafy environment. Cleafy managed firewall rules are reviewed quarterly. Customer shall be responsible for reviewing any Customer managed firewall rules on its instance(s).

5.3.5 Vulnerability Management. Cleafy conducts quarterly 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.

5.3.6 Antivirus. Cleafy updates antivirus, anti-malware, and anti-spyware software on regular intervals and centrally logs events for effectiveness of such software.

5.3.7 Change Control. Cleafy evaluates changes to platform, applications, and production infrastructure to minimize risk and such changes are implemented following Cleafy's standard operating procedure.

5.3.8 Data Separation. Customer Data shall be maintained within a logical single-tenant architecture on multi-tenant cloud infrastructure that is logically and physically separate from Cleafy's corporate infrastructure.

5.3.9 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.

5.3.10 Data Encryption in Transit. Cleafy shall use industry standard encryption to encrypt Customer Data in transit over public networks to the Subscription Service.

5.3.11 Data Encryption at Rest. Cleafy shall provide encryption at rest capability for full-disk encryption. This is done transparently without any changes to managed applications and without any actions on your part. Customer may purchase additional data-at-rest encryption capabilities if offered by Cleafy during the Subscription Term.

5.3.12 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.

5.3.13 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 its then current software vulnerability management program. Software patches are regularly made available to Customers to address known vulnerabilities.

5.3.14 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.

5.4 Organizational Security Measures

5.4.1 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.

5.4.2 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.

5.4.3 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.

5.4.4 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.

5.4.5 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.

5.4.6 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.

5.4.7 Mobile Devices Security. Cleafy shall implement and maintain security mechanisms on personnel mobile devices. Cleafy shall restrict personnel from disabling security mechanisms.

6. Service Continuity

6.1 Data Management & Data Backup. Cleafy will host the purchased instances of the Subscription Service in a pair of data centers that attained SSAE 18 Type 2 attestations or have ISO 27001 certifications (or equivalent or successor attestations or certifications) acting in an active/active capacity for the Subscription Term. Each data center includes full redundancy (N+1) and fault tolerant infrastructure for electrical, cooling and network systems. The deployed servers are enterprise scale servers with redundant power to ensure maximum uptime and service availability. The production database systems are replicated in near real time to a mirrored data center in a different geographic 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.

6.2 Disaster Recovery. Cleafy 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; (iii) make available 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.
6.3 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.

7. Monitoring and Incident Management

7.1 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.

7.2 Breach Notification. Cleafy will report to Customer any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data (a "Breach") without undue delay following determination by Cleafy that a Breach has occurred.

7.3 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 support 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.

7.4 Data Controller Obligations. Data Controller will cooperate with Data Processor in maintaining accurate contact information in the customer support portal 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.

7.5 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.

8. Penetration Tests

8.1 By a Third-Party. Cleafy contracts with third-party vendors to perform a penetration test on the Cleafy application per family release to identify risks and remediation options that help increase security. Cleafy shall make executive reports from the penetration testing available to Customer in Cleafy CORE.

8.2 By Customer. No more than once per calendar year Customer may request to perform, at its own expense, an application penetration test. Additional tests within a Release Family may be requested and if allowed, shall be subject to a fee. Prior to conducting any penetration test, Customer shall notify Cleafy by submitting a request to schedule such a test using the Support Portal per Cleafy's then-current penetration testing policy and procedure, including entering into Cleafy's penetration test agreement. Customer shall not perform a penetration test without Cleafy's express written authorization. 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 Subscription Service. Cleafy's approval for a Customer to perform a penetration test as set forth in this Section 6.2 includes the ability for Customer to retest the detected vulnerabilities from the initial penetration test.

9. Data Controller Monitoring Rights

9.1 Security Risk Assessment. Data Controller agrees that in accordance with Data Protection Laws and before submitting any Personal Data to the Subscription Service, Data Controller will perform an appropriate risk assessment to determine whether the security measures within the Subscription Service provide an adequate level of security, taking into account the nature, scope, context and purposes of the processing, the risks associated with the Personal Data and the applicable Data Protection Laws. Data Processor shall provide Data Controller reasonable assistance by providing Data Controller with information requested by Data Controller to conduct Data Controller's security risk assessment. Data Controller is solely responsible for determining the adequacy of the security measures within the Subscription Service in relation to the Personal Data Processed.

9.2 Certifications and Attestations. Cleafy shall establish and maintain sufficient controls to meet certification and attestation for the objectives stated in ISO 27001 and ISO 27018 (or equivalent standards) for the Security Program supporting the Subscription Service. At least once per calendar year, 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 Customer.

9.3 Audit. Data Processor shall allow for and contribute to audits that include inspections by granting Customer (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"). The information available in Cleafy CORE will include documentation evidencing Cleafy's Security Program, as well as Cleafy's privacy policies and procedures regarding personal information processed within the Subscription Service, copies of certifications and attestation reports (including audits) listed above.

9.4 Output. Upon completion of the Audit, Data Processor and Customer 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 Customer's suggested improvements noted in the Audit to improve Data Processor's Security Program. The Audit and the results derived therefrom are Confidential Information of Data Processor.

9.5 Data Controller Expenses. Any expenses incurred by Data Controller in connection with the Audit shall be borne exclusively by Data Controller.

10. Subprocessors

10.1 Use of Sub-Processors. Data Controller authorizes Data Processor to engage Sub-Processors appointed in accordance with this Section.

10.2 New Sub-Processors. Prior to Data Processor or a Data Processor Affiliate engaging a Sub-Processor, Data Processor shall: (a) notify Data Controller by email to Customer's designated contact(s) or by notification within the Support Portal (or other mechanism used to notify its customer base); and (b) ensure such Sub-Processor entered into a written agreement with Data Processor (or the relevant Data Processor Affiliate) requiring the Sub-Processor abide by terms no less protective than those provided in this DPA. Upon written request by Data Controller, Data Processor shall make a summary of the data processing terms available to Data Controller. Data Controller may request in writing reasonable additional information with respect to Sub-Processor's ability to perform the relevant Processing activities in accordance with this DPA.

10.3 Information about Sub-Processors. Information about Sub-Processors, including their functions and locations, is available at the Data Processor's Support Portal: "CLEAFY CLOUD PLATFORM SUBPROCESSORS.docx" (as may be updated by Cleafy from time to time in accordance with these Terms).

10.4 Right to Object. Data Controller may object to Data Processor's proposed use of a new Sub-Processor by notifying Data Processor within 10 days after receipt of Data Processor's notice if Data Controller reasonably determines - on the basis of grounded reasons - such Sub-Processor is unable to Process Personal Data in accordance with the terms of this DPA ("Objection Notice"). In the event Data Controller submits its Objection Notice, Data Processor shall reasonably consider such objection and will notify Data Controller if it intends to provide the applicable Subscription Service or Professional Services with the use of the Sub- Processor at issue ("Processor Notice"). Customer may terminate the applicable Order Form(s), Use Authorization(s) with respect to the Professional Service or Subscription Service requiring use of the Sub-Processor at issue upon written notice to Cleafy within 10 days of the date of Processor Notice ("Termination Period"). Cleafy will, as Customer's sole and exclusive remedy, refund to Customer any unused prepaid fees following the effective date of termination for the terminated services. For clarity, Data Processor will not engage the new Sub-Processor at issue until the expiration of the Termination Period.

10.5 Liability. Use of a Sub-Processor will not relieve, waive, or diminish any obligation of Data Processor under the Agreement, and Data Processor is liable for the acts and omissions of any Sub-Processor to the same extent as if the acts or omissions were performed by Data Processor.

11. Requests made from Data Subjects and Authorities

11.1 Requests from Data Subjects. During the Subscription Term, Data Processor shall provide Data Controller with the ability to access, correct, rectify, erase, or block Personal Data, or to transfer or port such Personal Data, within the Subscription Service, as may be required under Data Protection Laws (collectively, "Data Subject Requests").

11.2 Responses. 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 Data Subject Requests to the extent Data Controller is unable to fulfill such Data Subject Requests using the functionality in the Subscription Service. Data Processor will instruct the Data Subject to contact the Customer in the event Data Processor receives a Data Subject Request directly.

11.3 Requests from Authorities. 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 Personal Data, Data Processor shall promptly notify 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.

10.Data Transfer

The Data Processor may not transfer or authorize the transfer of Data to countries outside the EU and/or the European Economic Area (EEA) without the prior written consent of Controller. If personal data processed under this Agreement is transferred from a country within the European Economic Area to a country outside the European Economic Area, the Parties shall ensure that the personal data are

adequately protected. To achieve this, the Parties shall, unless agreed otherwise, rely on EU approved standard contractual clauses for the transfer of personal data.

13. General Terms

13.1 Confidentiality. Each Party must keep any information it receives about the other Party and its business in connection with this Agreement ("Confidential Information") confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that (a) disclosure is required by law and (b) the relevant information is already in the public domain.

13.2 Customer's Affiliates. The obligations of Data Processor set forth herein will extend to Customer's Data Controller Affiliates to which Customer provides access to the Subscription Service or whose Personal Data is Processed within the Subscription Service, subject to the following conditions:

13.2.1 Compliance. Customer shall at all times be liable for its Affiliates' compliance with this DPSA and all acts and omissions by a Data Controller Affiliate are considered acts and omissions of Customer.

13.2.2 Claims. Customer's Data Controller Affiliates will not bring a claim directly against Data Processor. In the event a Data Controller Affiliate wishes to assert a valid legal action, suit, claim or proceeding against Data Processor (a "Data Controller Affiliate Claim"): (i) Customer must bring such Data Controller Affiliate Claim directly against Data Processor on behalf of such Data Controller Affiliate, unless Data Protection Laws require that Data Controller Affiliate be party to such Data Controller Affiliate Claim; and (ii) all Data Controller Affiliate Claims will be considered claims made by Customer and are at all times subject to any aggregate limitation of liability set forth in the Agreement

13.2.3 Data Controller Affiliate Ordering. If a Data Controller Affiliate purchased a separate instance of the Subscription Service under the terms of the signed master agreement between Cleafy and Customer, then such Data Controller Affiliate will be deemed a party to this DPA and shall be treated as Customer under the terms of this DPA.

13.3 Product Capabilities. The Subscription Service allows Customer to: (a) authenticate users before accessing the Customer's instance; (b) integrate with SAML solutions (c) encrypt passwords; (d) allow users to manage passwords; and (e) prevent access by users with an inactive account. Customer manages each user's access to and use of the Subscription Service by assigning to each user a credential and user type that controls the level of access to the Subscription Service. Customer is solely responsible for reviewing Cleafy's Security Program and making an independent determination as to whether it meets Customer's requirements, taking into account the type and sensitivity of Customer Data that Customer processes within the Subscription Service. Customer shall be responsible for implementing encryption and access control functionalities available within the Subscription Service for protecting all Customer Data containing sensitive data, including credit card numbers, social security and other government-issued identification numbers, financial and health information, Personal Data (including any data deemed sensitive or "special categories of personal data" under Data Protection Laws). Customer is solely responsible for its decision not to encrypt such Customer Data and Cleafy will have no liability to the extent that damages would have been mitigated by Customer's use of such encryption measures. Customer is responsible for protecting the confidentiality of each user's login and password and managing each user's access to the Subscription Service. Customer shall be responsible for implementing Cleafy's documented best practices and hardening guidelines for securing its Cleafy instances.

13.4 Security Contact. Customer agrees to identify and maintain appropriate security contact(s) for all information security incident and information security-related communication within the Support Portal.

13.4.1 Customer Authorized Contacts. Customer will appoint a reasonable number of contacts ("Customer Authorized Contacts") to engage Customer Support for questions and technical issues and Customer must maintain current contact information for the authorized contacts in the Support Portal who have been trained to administer the Subscription Service.

13.5 Notices. All notices and communications given under this Agreement must be in writing and will

be sent by email. Controller shall be notified by email sent to the address related to its use of the Service under the Principal Agreement. Processor shall be notified by email sent to the address: privacy@cleafy.com.

13.6 Limitations. Notwithstanding anything to the contrary in this DSA or other parts of the Agreement, Cleafy's obligations herein are only applicable to the Subscription Service. This DPSA does not apply to: (a) information shared with Cleafy that is not Customer Data; (b) data in Customer's VPN or a third-party network; and (c) any data processed by Customer or its users in violation of the Agreement or this DPSA. Moreover, Customer is responsible for its use of the Services and its storage of any copies of Customer Data outside Cleafy's or Cleafy's Subprocessors' systems, including:

- using the Services and Additional Security Controls to ensure a level of security appropriate to the risk in respect of the Customer Data;
- securing the account authentication credentials, systems and devices Customer uses to access the Services; and
- backing up its Customer Data as appropriate.

13.7 Entire agreement. This Agreement sets forth the entire agreement and understanding of the parties relating to the subject matter herein and supersedes all prior or contemporaneous discussions, understandings and agreements, whether oral or written, between them relating to the subject matter hereof.

13.8 Severability. The invalidity or unenforceability of any particular provision of this Agreement shall not affect the other provisions, and this Agreement shall be construed in all respects as if any invalid or unenforceable provision were omitted or limited to the minimum extent necessary for this Agreement otherwise to remain enforceable in full force and effect.

13.9 Amendments. No modification of or amendment to this Agreement, nor any waiver of any rights under this Agreement, shall be effective unless in writing signed by the parties to this Agreement. No delay or failure to require performance of any provision of this Agreement shall constitute a waiver of that provision as to that or any other instance.

14 Liability limitations and exclusions

14.1 Subject to no exceptions whatsoever, either Party shall be fully liable for damages (i) caused by intent or gross negligence, (ii) and for damages to life, limb or health, and (iii) subject to mandatory liability by law.

14.2. Provided not explicitly stated otherwise in this Agreement, either Party's liability towards the other Party under any theory of law for all damages and/or expenses and/or losses caused from all slightly negligent acts shall be limited for all slightly negligent act(s) to a maximum of one hundred (100%) of the cumulated sum of net invoice amounts of all invoices issued by Cleafy spa under this Agreement within a twelve (12) months period preceding the occurrence of the last of such slightly negligent acts. For the avoidance of doubt, in case the slightly negligent act arises within the first twelve (12) months period after the Effective Date then the cumulated sum of net invoice amounts of all invoices issued by Cleafy spa under this Agreement prior to occurrence of this slightly negligent act will be used to calculate the respective sum of the net invoice amount. The liability of either Party for all indirect, special, consequential, punitive or exemplary damages, loss of profit, loss of business opportunities, loss of revenues, lost savings and loss of goodwill shall be in any cases excluded.

14.3 The liability of either Party for damages caused by neither intent nor negligence under any theory of law shall be excluded.

14.4 If permits, rights or licenses are either granted with delay or not granted by authorities, any liability for resulting losses and claims against either Party shall be excluded.

14.5 The liability of either Party according to any law that imposes mandatory liability remains unaffected by all provisions of this Agreement.

14.6 Paragraphs (1) through (5) of this section shall apply mutatis mutandis to the personal liability of

Cleafy Spa directors, officers, agents, employees, contractors and Subcontractors.

15. Jurisdiction and venue

The validity, construction and performance of this Agreement shall be governed by the laws of Italy, without regard to the laws as to choice or conflict of laws. If disputes arise in connection with this Agreement, the Parties shall make every effort to settle them amicably. If the Parties were unable to reach an agreement even after exhausting an escalation option, the parties were refer exclusively to the Courts in Milano (Italy).