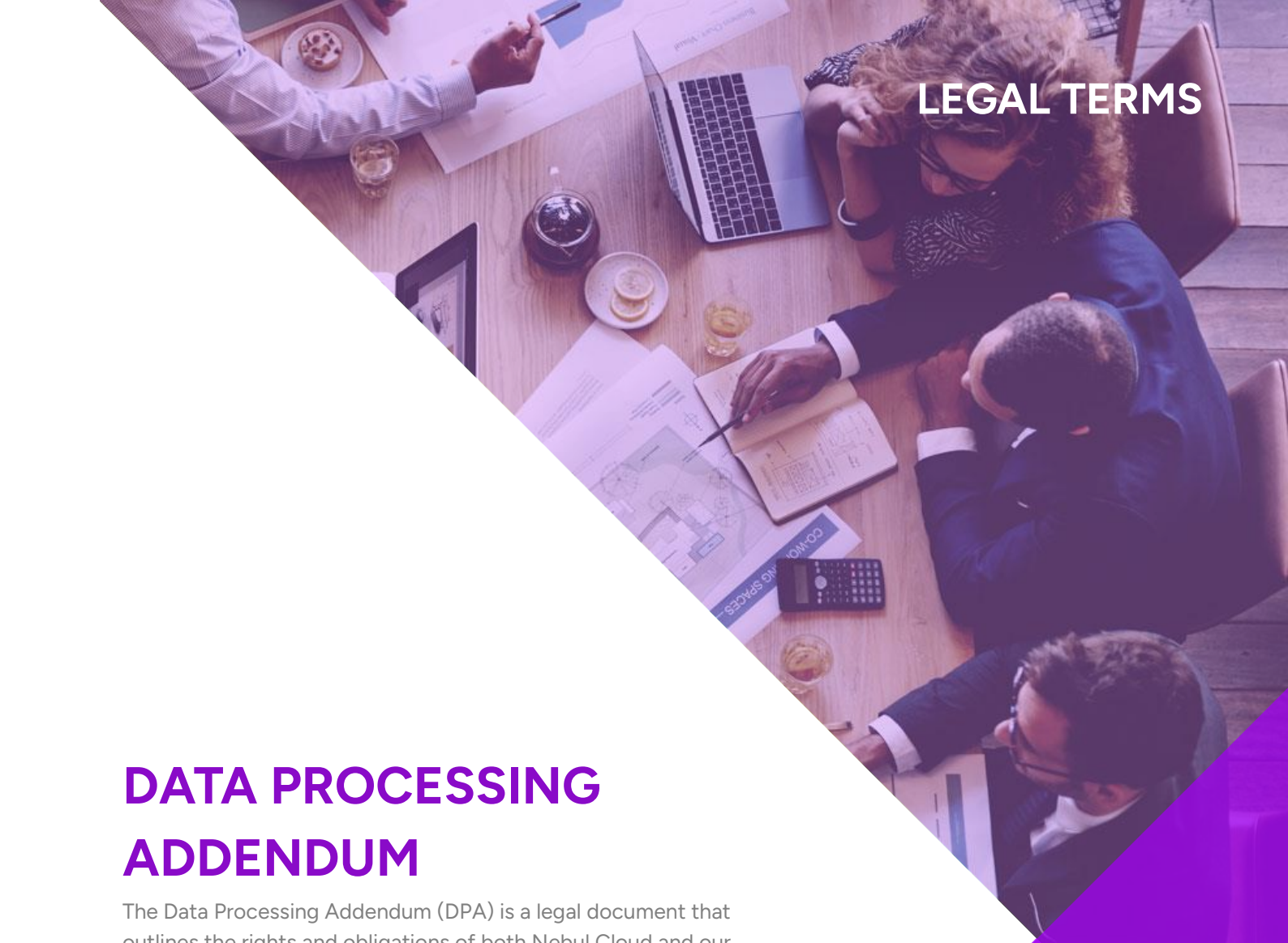

LEGAL TERMS

DATA PROCESSING ADDENDUM

The Data Processing Addendum (DPA) is a legal document that outlines the rights and obligations of both Nebul Cloud and our customers regarding the processing and protection of personal data. This addendum ensures compliance with applicable privacy laws, including the GDPR, and sets clear guidelines for how customer data is handled, stored, and secured. It is an integral part of our commitment to maintaining the highest standards of data privacy and security.

Latest updated: June 2024

Table of Contents

Schedules

Data Processing Addendum (Customers)

This Data Processing Addendum (including its appendices, the "Addendum") is incorporated into the Agreement(s) (as defined below) between Nebul and Customer.

1 OVERVIEW

This Addendum describes the parties' obligations, including under applicable privacy, data security, and data protection laws, with respect to the processing and security of Customer Data (as defined below). This Addendum will be effective on the Addendum Effective Date (as defined below), and will replace any terms previously applicable to the processing and security of Customer Data. Capitalized terms used but not defined in this Addendum have the meaning given to them in the Agreement.

2 DURATION

This Addendum will remain in effect until, and automatically expire when the Agreement has been terminated and Nebul has deleted all Customer Data in accordance with this Addendum.

3 ROLES; LEGAL COMPLIANCE

3.1 Roles of Parties. Nebul is a processor and Customer is a controller or processor, as applicable, of Customer Personal Data.

3.2 Processing Summary. The subject matter and details of the processing of Customer Personal Data are described in Schedule 2 (Subject Matter and Details of Data Processing).

3.3 Compliance with Law. Each party will comply with its obligations related to the processing of Customer Personal Data under Applicable Privacy Law.

4 DATA PROCESSING

4.1 Processor Customers. If Customer is a processor:

A) Customer warrants on an ongoing basis that the relevant controller has authorized:

i. the Instructions;

ii. Customer's engagement of Nebul as another processor; and

iii. Nebul's engagement of Subprocessors as described in Section 10 (Subprocessors);

B) Customer will forward to the relevant controller promptly and without undue delay any notice provided by Nebul under Section 6.2.1 (Incident Notification), 8.2.1 (Responsibility for Requests), or 10.4 (Opportunity to Object to Subprocessors); and

C) Customer may make available to the relevant controller any other information made available by Nebul under this Addendum about the locations of Nebul data centers or the names, locations, and activities of Subprocessors.

4.2 Compliance with Customer's Instructions. Customer instructs Nebul to only process Customer Data in accordance with the Agreement (including this Addendum) and applicable law only as follows:

A) to provide, secure, and monitor the Services and Technical Support Services (if applicable); and

B) is further specified via:

i. Customer's use of the Services (including via the Customer Portal) and Technical Support Services (if applicable); and

ii. Any other written instructions given by Customer and acknowledged by Nebul as constituting instructions under this Addendum (collectively, the "Instructions").

4.3 Nebul will comply with the Instructions unless prohibited by Dutch Law, European Data Protection Law or, where applicable, prohibited by any other Applicable Privacy Law. in which case Nebul will immediately notify Customer before processing Customer Data.

4.4 Nebul will refrain from processing Customer data on any other ground than the Instructions unless legally required to do so by Dutch or European Data Protection Law. Nebul will inform Customer of this legal requirement unless prohibited to do so important grounds of public interest.

5 DATA DELETION

5.1 Deletion by Customer. Nebul will enable Customer to delete Customer Data during the Term in a manner consistent with the functionality of the Services. If Customer uses the Services to delete any Customer Data during the Term and that Customer Data cannot be recovered by Customer, this use will constitute an Instruction to Nebul to delete the relevant Customer Data from Nebul's systems in accordance with applicable law. Nebul will comply with this Instruction as soon as reasonably practicable and within a maximum period of 180 days, unless European Law or, where applicable, Applicable Privacy Law requires longer retention of Customer Data.

5.2 Return or Deletion When Term Ends. Customer instructs Nebul to delete all remaining Customer Data (including existing copies) from Nebul's systems in accordance with Applicable Privacy Law when the Agreement has been terminated and the Term initiates. After a recovery period of up to 30 days from the Term, Nebul will comply with this Instruction as soon as reasonably practicable and within a maximum period of 180 days, unless European Law or, where applicable, any other Applicable Privacy Law requires longer retention of Customer Data, of which requirement Nebul will inform Customer. If Customer wishes to retain any Customer Data after the end of the Term, it may instruct Nebul in accordance with Section 8.1 (Access; Rectification; Restricted Processing; Portability) to return that data during the Term. Subject to Section 5.3 (Deferred Deletion Instruction).

5.3 Deferred Deletion Instruction. To the extent any Customer Data covered by the deletion instruction described in Section 5.2 (Return or Deletion When Term Ends) is also processed when the applicable Term under Section 5.2 expires, in relation to an Agreement with a continuing Term, such deletion instruction will take effect with respect to such Customer Data only when the continuing Term expires. For clarity, this Addendum will continue to apply to such Customer Data until its deletion by Nebul.

6 DATA SECURITY

6.1 Nebul's Security Measures, Controls, and Assistance.

6.1.1 Nebul's Security Measures. Nebul will implement and maintain appropriate technical, organizational, and physical measures to ensure the security of processing Customer Data and to adequately protect Customer Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access as described in Schedule 3 (Security Measures) (the "Security Measures"). The Security Measures include measures to encrypt Customer Data; to help ensure ongoing confidentiality, integrity, availability and resilience of Nebul's systems and services; to help restore timely access to Customer Data following an incident; and for regular testing of effectiveness. Nebul may update the Security Measures from time to time provided that such updates do not result in a material reduction of the security of the Services.

6.1.2 Access and Compliance. Nebul will:

A) authorize its employees, contractors, and Subprocessors to access Customer Data only as strictly necessary to comply with Instructions;

B) take appropriate steps to ensure compliance with the Security Measures by its employees, contractors, and Subprocessors to the extent applicable to their scope of performance; and

C) ensure that all persons authorized to process Customer Data are under a contractual obligation of confidentiality.

6.1.3 Additional Security Controls. Nebul will make Additional Security Controls available to:

A) allow Customer to take steps to secure Customer Data; and

B) provide Customer with information about securing, accessing, and using Customer Data.

6.1.4 Nebul's Security Assistance. Nebul will (taking into account the nature of the processing of Customer Personal Data and the information available to Nebul) assist Customer in ensuring compliance with its (or, where Customer is a processor, the relevant controller's) obligations relating to security and personal data breaches under Applicable Privacy Law, by:

A) implementing and maintaining the Security Measures in accordance with Section 6.1.1 (Nebul's Security Measures);

B) making Additional Security Controls available in accordance with Section 6.1.3 (Additional Security Controls);

C) complying with the terms of Section 6.2 (Data Incidents); and

D) making the Security Documentation available in accordance with Section 6.5.1 (Reviews of Security Documentation) and providing the information contained in the applicable Agreement (including this Addendum).

6.2 Data Incidents.

6.2.1 Incident Notification. Nebul will notify Customer promptly and without undue delay after becoming aware of a Data Incident, and promptly take reasonable steps to minimize harm and secure Customer Data.

6.2.2 Details of Data Incident. Nebul's notification of a Data Incident will describe: the nature of the Data Incident including the Customer resources impacted; the measures Nebul has taken, or plans to take, to address the Data Incident and mitigate its potential risk; the measures, if any, Nebul recommends that Customer take to address the Data Incident; and details of a contact point where more information can be obtained. If it is not possible to provide all such information at the same time, Nebul's initial notification will contain the information then available and further information will be provided without undue delay as it becomes available.

6.2.3 No Assessment of Customer Data by Nebul. Nebul has no obligation to assess Customer Data in order to identify information subject to any specific legal requirements.

6.2.4 No Acknowledgement of Fault by Nebul. Nebul's notification of or response to a Data Incident under this Section 6.2 (Data Incidents) will not be construed as an acknowledgement by Nebul of any fault or liability with respect to the Data Incident.

6.2.5 Notification to the Supervisory Authority. Nebul will (taking into account the nature of the processing and the information available to Nebul) assist Customer in notifying the Data Incident to the competent Supervisory Authority(ies). The responsibility of notifying the Data Incident is exclusively reserved for the Customer or, if the Customer is a processor, the relevant controller.

6.3 Customer's Security Responsibilities and Assessment.

6.3.1 Customer's Security Responsibilities. Without prejudice to Nebul's obligations under Sections 6.1 (Nebul's Security Measures, Controls and Assistance) and 6.2 (Data Incidents), and elsewhere in the applicable Agreement, Customer is responsible for its use of the Services and its storage of any copies of Customer Data outside Nebul's or Nebul's Subprocessors' systems, including:

A) using the Services and Additional Security Controls to ensure a level of security appropriate to the risk to the Customer Data;

B) securing the account authentication credentials, systems, and devices Customer uses to access the Services; and

C) backing up or retaining copies of its Customer Data as appropriate.

6.3.2 Customer's Security Assessment. Customer agrees that the Services, Security Measures, Additional Security Controls, and Nebul's commitments under this Section 6 (Data Security) provide a level of security appropriate to the risk to Customer Data (taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of the processing of Customer Data as well as the risks to individuals).

6.4 Compliance Certifications and SOC Reports. Nebul will maintain at least the following for the Audited Services to verify the continued effectiveness of the Security Measures:

A) certificates for ISO 27001 ("Compliance Certifications"); and

B) SOC 2 reports produced by Nebul's Third-Party Auditor and updated annually based on an audit performed at least once every 12 months (the "SOC Reports").

Nebul may add standards at any time. Nebul may replace a Compliance Certification or SOC Report with an equivalent or enhanced alternative.

6.5 Reviews and Audits of Compliance.

6.5.1 Reviews of Security Documentation. To demonstrate compliance by Nebul with its obligations under this Addendum, Nebul will make the information necessary to demonstrate compliance with the Addendum available for review upon request from the Customer and, if Customer is a processor, allow Customer to request access to the SOC Reports for the relevant controller in accordance with Section 6.5.3 (Additional Business Terms for Reviews and Audits).

6.5.2 Customer's Audit Rights.

A) Customer Audit. Nebul will, if required under Applicable Privacy Law, allow Customer or an independent auditor appointed by Customer to conduct audits (including inspections) to verify Nebul's compliance with its obligations under this Addendum in accordance with Section 6.5.3 (Additional Business Terms for Reviews and Audits). During an audit, Nebul will reasonably cooperate with Customer or its auditor as described in this Section 6.5 (Reviews and Audits of Compliance).

B) Customer Independent Review. Customer may conduct an audit to verify Nebul's compliance with its obligations under this Addendum by reviewing the Security Documentation (which reflects the outcome of audits conducted by Nebul's Third-Party Auditor).

6.5.3 Additional Business Terms for Reviews and Audits.

A) Customer must contact Nebul's Data Protection Team to request:

i. access to the SOC Reports for a relevant controller under Section 6.5.1 (Reviews of Security Documentation

ii. an audit under Section 6.5.2(a) (Customer Audit).

B) Following a Customer request under Section 6.5.3(a), Nebul and Customer will discuss and agree in advance on:

i. security and confidentiality controls applicable to any access to the SOC Reports by a relevant controller under Section 6.5.1 (Reviews of Security Documentation); and

ii. The reasonable start date, scope, and duration of and security and confidentiality controls applicable to any audit under Section 6.5.2(a) (Customer Audit).

C) Nebul may charge a fee (based on Nebul's reasonable costs) for any access request to the SOC Reports under Section 6.5.1. Nebul will provide Customer with further details of any applicable fee, and the basis of its calculation, in advance of any such request.

D) The costs of any audit under Section 6.5.2 will be borne by the Customer. Customer will be responsible for the payment of any fees charged by any auditor appointed by Customer to execute any such audit.

E) Nebul may object in writing to an auditor appointed by Customer to conduct any audit under Section 6.5.2(a) (Customer Audit) if the auditor is, in Nebul's reasonable opinion, not suitably qualified or independent, a competitor of Nebul, or otherwise manifestly unsuitable. Any such objection by Nebul will require Customer to appoint another auditor or conduct the audit itself.

7 IMPACT ASSESSMENTS AND CONSULTATIONS

Nebul will (taking into account the nature of the processing and the information available to Nebul) assist Customer in ensuring compliance with its (or, where Customer is a processor, the relevant controller's) obligations relating to data protection impact assessments, risk assessments, prior consultations with the Competent Supervisory Authority or equivalent procedures under Applicable Privacy Law, by:

A) making Additional Security Controls available in accordance with Section 6.1.3 (Additional Security Controls) and the Security Documentation available in accordance with Section 6.5.1 (Reviews of Security Documentation);

B) providing the information contained in the applicable Agreement (including this Addendum); and

C) if subsections (a) and (b) above are insufficient for Customer (or the relevant controller) to comply with such obligations, upon Customer's request, providing Customer with additional reasonable cooperation and assistance.

8 ACCESS; DATA SUBJECT RIGHTS

8.1 Access; Rectification; Restricted Processing; Portability. During the Term, Nebul will implement and maintain technical, organizational, and physical measures to enable Customer, in a manner consistent with the functionality of the Services, to access, rectify, and restrict processing of Customer Data, including via the deletion functionality provided by Nebul as described in Section 5.1 (Deletion by Customer), and to export Customer Data. If Customer becomes aware that any Customer Personal Data is inaccurate or outdated, Customer will be responsible for using such functionality to rectify or delete that data if required by Applicable Privacy Law.

8.2 Data Subject Requests.

8.2.1 Responsibility for Requests. During the Term, if Nebul's Cloud Data Protection Team receives a request from a data subject that relates to Customer Personal Data and identifies Customer, Nebul will:

A) promptly notify Customer; and

B) not respond to that data subject's request without authorization from Customer.

Customer will be responsible for responding to any such request including, where necessary, by using the functionality of the Services.

8.2.2 Nebul's Data Subject Request Assistance. Nebul will (taking into account the nature of the processing of Customer Personal Data) assist Customer in fulfilling its (or, where Customer is a processor, the relevant controller's) obligations under Chapter III of the GDPR in responding to requests for exercising the data subject's rights by:

A) making Additional Security Controls available in accordance with Section 6.1.3 (Additional Security Controls);

B) complying with Sections 8.1 (Access; Rectification; Restricted Processing; Portability) and 8.2.1 (Responsibility for Requests); and

C) if subsections (a) and (b) above are insufficient for Customer (or the relevant controller) to comply with such obligations, upon Customer's request, providing Customer with additional reasonable cooperation and assistance.

9 DATA PROCESSING LOCATIONS

9.1 Data Storage and Processing Facilities. Subject to Nebul's data location commitments all Customer data will remain within the EU in terms of Location, Control and Operations. Customer Data may be processed in any country where Nebul or its Subprocessors maintain facilities.

9.2 Data Center Information. The locations of Nebul data centers are described in Schedule 4 (Datacenter locations).

10 SUBPROCESSORS

10.1 Consent to Subprocessor Engagement. Customer specifically authorizes Nebul's engagement as Subprocessors of those entities disclosed as described in Section 10.2 (Information about Subprocessors) as of the Addendum Effective Date. In addition, without prejudice to Section 10.4 (Opportunity to Object to Subprocessors), Customer generally authorizes Nebul's engagement of other third parties as Subprocessors ("New Subprocessors").

10.2 Information about Subprocessors. Names, locations, and activities of Subprocessors are described in Schedule 4 (Subprocessors).

10.3 Requirements for Subprocessor Engagement. When engaging any Subprocessor, Nebul will:

A) ensure via a written contract that:

i. the Subprocessor only accesses and uses Customer Data to the extent required to perform the obligations pursuant to the agreement concluded with Nebul, and does so in accordance with the applicable Agreement (including this Addendum); and

ii. the data protection obligations described in this Addendum are imposed on the Subprocessor; and

B) remain fully liable for all obligations subcontracted to, and all acts and omissions of, the Subprocessor.

10.4 Opportunity to Object to Subprocessors.

A) When Nebul engages any New Subprocessor during the Term, Nebul will, at least 30 days before the New Subprocessor starts processing any Customer Data, notify Customer of the engagement (including the name, location, and activities of the New Subprocessor).

B) Customer may, within 15 days after being notified of the engagement of a new Subprocessor, object to the engagement by Nebul of the New Subprocessor. Parties will then in good faith discuss possible solutions. If Parties cannot reach an agreement, the Customer may terminate the Agreement and all Service Contracts. In that case all fees for the remainder of the Service Contracts in place at the time of termination will become immediately due and payable.

11 SAFE DATA PROTECTION; PROCESSING RECORDS

11.1 SAFE Data Protection. Nebul's SAFE Data Protection Service Team will provide prompt and reasonable assistance with any Customer queries related to the processing of Customer Data under the applicable Agreement and can be contacted as described in the Notices section of the applicable Agreement.

11.2 Nebul's Processing Records. Nebul will keep appropriate documentation of its processing activities as required by Applicable Privacy Law. To the extent any Applicable Privacy Law requires Nebul to collect and maintain records of certain information relating to Customer, Customer will use the Customer Portal to supply such information and keep it accurate and up-to-date. Nebul may make any such information available to competent regulators, including a Supervisory Authority, if required by Applicable Privacy Law.

11.3 Controller Requests. During the Term, if Nebul receives a request or instruction from a third party purporting to be a controller of Customer Personal Data, Nebul will advise the third party to contact Customer.

12 NOTICES

Notices under this Addendum (including notifications of any Data Incidents) will be delivered to the Notification Email Address. Customer is responsible for using the Customer Portal to ensure that its Notification Email Address remains current and valid.

13 GENERAL

13.1 Governing Law. This Addendum and any dispute of any sort that might arise between Nebul and Customer is governed by Dutch law, without prejudice to its conflicts of law rules.

13.2 Competent court. All disputes that may arise out of or in connection with this Addendum, or with any Agreement, entered into pursuant hereto or in furtherance hereof, shall be brought exclusively before the competent court according to the Agreement.

Schedule 1. Definitions

1. Definitions in this agreement:

- **"Addendum Effective Date"** means the date on which Customer accepted, or the parties otherwise agreed to, this Addendum.
- **"Additional Security Controls"** means security resources, features, functionality, and controls that Customer may use at its option and as it determines, including the Customer Portal, encryption, logging and monitoring, identity and access management, security scanning, and firewalls.
- **"Agreement"** means the contract under which Nebul has agreed to provide the applicable Services to Customer.
- **"Applicable Privacy Law"** means, as applicable to the processing of Customer Personal Data, any national, federal, European Union, state, provincial or other privacy, data security, or data protection law or regulation.
- **"Audited Services"** means the then-current Services indicated as being in-scope for the relevant certification or report. Nebul may not remove any Services from this URL unless they have been discontinued in accordance with the applicable Agreement.
- **"Compliance Certifications"** has the meaning given in Section 6.4 (Compliance Certifications and SOC Reports).
- **"Customer Data"** means data provided to Nebul by Customer or End Users through Nebul Cloud Platform under the Customer Account, and data that Customer or End Users derive from that data through their use of Nebul Cloud.
- **"Customer Personal Data"** means the personal data contained within the Customer Data, including any special categories of personal data or sensitive data defined under Applicable Privacy Law.
- **"Data Incident"** means a breach of Nebul's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data on systems managed by or otherwise controlled by Nebul.
- **"EMEA"** means Europe, the Middle East, and Africa.
- **"EU GDPR"** means 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.
- **"European Data Protection Law"** means, as applicable: (a) the GDPR; or (b) the Swiss FADP.
- **"European Law" means, as applicable:** (a) EU or EU Member State law (if the EU GDPR applies to the processing of Customer Personal Data); (b) the law of the UK or a part of the UK (if the UK GDPR applies to the processing of Customer Personal Data); or (c) the law of Switzerland (if the Swiss FADP applies to the processing of Customer Personal Data).
- **"GDPR"** means, as applicable: (a) the EU GDPR; or (b) the UK GDPR.
- **"Nebul's Third-Party Auditor"** means a Nebul-appointed, qualified, and independent third-party auditor, whose then-current identity Nebul will disclose to Customer.
- **"Instructions"** has the meaning given in Section 4.2 (Compliance with Customer's Instructions).
- **"Notification Email Address"** means the email address(es) designated by Customer in the Customer Portal or Order Form to receive certain notifications from Nebul.
- **"Security Documentation"** means the Compliance Certifications and the SOC Reports.
- **"Security Measures"** has the meaning given in Section 6.1.1 (Nebul's Security Measures).
- **"Services"** means the applicable services described in Appendix 4 (Specific Products).
- **"SOC Reports"** has the meaning given in Section 6.4 (Compliance Certifications and SOC Reports).
- **"Subprocessor"** means a third party authorized as another processor under this Addendum to process Customer Data to provide parts of the Services and Technical Support Services (if applicable).
- **"Supervisory Authority"** means, as applicable: (a) a "supervisory authority" as defined in the EU GDPR; or (b) the "Commissioner" as defined in the UK GDPR or the Swiss FADP.

- **"Swiss FADP"** means, as applicable, the Federal Act on Data Protection of 19 June 1992 (Switzerland) (with the Ordinance to the Federal Act on Data Protection of 14 June 1993) or the revised Federal Act on Data Protection of 25 September 2020 (Switzerland) (with the Ordinance to the Federal Act on Data Protection of 31 August 2022).
- **"Term"** means the period from the Addendum Effective Date until the end of the Agreement including, if applicable, any period during which the provision of the Services may be suspended and any post-termination period during which Nebul may continue providing the Services for transitional purposes.
- **"UK GDPR"** means the EU GDPR as amended and incorporated into UK law under the UK European Union (Withdrawal) Act 2018, and applicable secondary legislation made under that Act.

2. Terms:

2.1 The terms "personal data", "data subject", "processing", "controller", and "processor" as used in this Addendum have the meanings given by the EU GDPR.

Schedule 2: Subject Matter and Details of Data Processing

Subject Matter
Nebul's provision of the Services and Technical Support Services (if applicable) to Customer.

Duration of the Processing
The Term plus the period from the end of the Term until deletion of all Customer Data by Nebul in accordance with this Addendum.

Nature and Purpose of the Processing
Nebul will process Customer Personal Data for the purposes of providing the Services and Technical Support Services (if applicable) to Customer in accordance with this Addendum.

Categories of Data
Customer Personal Data provided to Nebul via the Services, by (or at the direction of) Customer (or its End Users).

Data Subjects
Data subjects include the individuals about whom Customer Personal Data is provided to Nebul via the Services by (or at the direction of) Customer or by its End Users.

Schedule 3: Security Measures

As from the Addendum Effective Date, Nebul will implement and maintain the Security Measures described in this Schedule 3.

1. Data Center and Network Security

(A) Data Centers.

- **Infrastructure.** Nebul maintains geographically distributed data centers. Nebul stores all production data in physically secure data centers.
- **Redundancy.** Infrastructure systems are designed to eliminate single points of failure and minimize the impact of anticipated environmental risks. Dual circuits, switches, networks, or other necessary devices provide this redundancy. The Services are designed to allow Nebul to perform certain types of preventative and corrective maintenance without interruption. All environmental equipment and facilities have documented preventative maintenance procedures that detail the process for and frequency of performance in accordance with the manufacturer's or internal specifications. Preventative and corrective maintenance of the data center equipment is scheduled through a standard change process according to documented procedures.
- **Power.** The data center electrical power systems are designed to be redundant and maintainable without impacting continuous operations, 24 hours a day, 7 days a week. In most cases, a primary as well as an alternate power source, each with equal capacity, is provided for critical infrastructure components in the data center. Backup power is provided by various mechanisms such as uninterruptible power supplies (UPS) batteries, which supply consistently reliable power protection during utility brownouts, blackouts, overvoltage, undervoltage, and out-of-tolerance frequency conditions. If utility power is interrupted, backup power is designed to provide transitory power to the data center, at full capacity, for up to 10 minutes until the backup generator systems take over. The backup generators are capable of automatically starting up within seconds to provide enough emergency electrical power to run the data center at full capacity typically for a period of days.
- **Server Operating Systems.** Nebul servers use a Linux-based implementation customized for the application environment. Data is stored using proprietary algorithms to augment data security and redundancy.
- **Code Quality.** Nebul employs a code review process to increase the security of the code used to provide the Services and enhance the security of products in production environments.
- **Business Continuity.** Nebul has designed and regularly plans and tests its business continuity planning/disaster recovery programs.

(B) Networks and Transmission.

- **Data Transmission.** Data centers are typically connected via high-speed private links to provide secure and fast data transfer between data centers. This is designed to prevent data from being read, copied, altered, or removed without authorization during electronic transfer or transport or while being recorded onto data storage media. Nebul transfers data via Internet standard protocols.
- **External Attack Surface.** Nebul employs multiple layers of network devices and intrusion detection to protect its external attack surface. Nebul considers potential attack vectors and incorporates appropriate purpose-built technologies into external-facing systems.
- **Intrusion Detection.** Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents. Nebul's intrusion detection involves: (i) tightly controlling the size and make-up of Nebul's attack surface through preventative measures; (ii) employing intelligent detection controls at data entry

points; and (iii) employing technologies that automatically remedy certain dangerous situations.

- **Incident Response.** Nebul monitors a variety of communication channels for security incidents, and Nebul's security personnel will react promptly to known incidents.
- **Encryption Technologies.** Nebul makes HTTPS encryption (also referred to as SSL or TLS connection) available. Nebul servers support ephemeral elliptic curve Diffie-Hellman cryptographic key exchange signed with RSA and ECDSA. These perfect forward secrecy (PFS) methods help protect traffic and minimize the impact of a compromised key, or a cryptographic breakthrough.

2. Access and Site Controls

(A) Site Controls.

- On-site Data Center Security Operation. Nebul's data centers maintain an on-site security operation responsible for all physical data center security functions 24 hours a day, 7 days a week. The on-site security operation personnel monitor closed-circuit TV (CCTV) cameras and all alarm systems. On-site security operation personnel perform internal and external patrols of the data center regularly.
- Data Center Access Procedures. Nebul maintains formal access procedures for allowing physical access to the data centers. The data centers are housed in facilities that require electronic card key access, with alarms that are linked to the on-site security operation. All entrants to the data center are required to identify themselves as well as show proof of identity to on-site security operations. Only authorized employees, contractors, and visitors are allowed entry to the data centers. Only authorized employees and contractors are permitted to request electronic card key access to these facilities. Data center electronic card key access requests must be made through e-mail, and require the approval of the requestor's manager and the data center director. All other entrants requiring temporary data center access must: (i) obtain approval in advance from the data center managers for the specific data center and internal areas they wish to visit; (ii) sign in at on-site security operations; and (iii) reference an approved data center access record identifying the individual as approved.
- On-site Data Center Security Devices. Nebul's data centers employ a dual authentication access control system that is linked to a system alarm. The access control system monitors and records each individual's electronic card key and when they access perimeter doors, shipping and receiving, and other critical areas. Unauthorized activity and failed access attempts are logged by the access control system and investigated, as appropriate. Authorized access throughout the business operations and data centers is restricted based on zones and the individual's job responsibilities. The fire doors at the data centers are alarmed. CCTV cameras are in operation both inside and outside the data centers. The positioning of the cameras has been designed to cover strategic areas including, among others, the perimeter, doors to the data center building, and shipping/receiving. On-site security operations personnel manage the CCTV monitoring, recording, and control equipment. Secure cables throughout the data centers connect the CCTV equipment. Cameras record on-site via digital video recorders 24 hours a day, 7 days a week. The surveillance records are retained for up to 30 days based on activity.

(B) Access Control.

- Infrastructure Security Personnel. Nebul has, and maintains, a security policy for its personnel, and requires security training as part of the training package for its personnel. Nebul's infrastructure security personnel are responsible for the ongoing monitoring of Nebul's security infrastructure, the review of the Services, and responding to security incidents.

- Access Control and Privilege Management. Customer's Administrators and End Users must authenticate themselves via a central authentication system or via a single sign-on system to use the Services.
- Internal Data Access Processes and Policies – Access Policy. Nebul's internal data access processes and policies are designed to prevent unauthorized persons and systems from gaining access to systems used to process Customer Data. Nebul designs its systems to (i) only allow authorized persons to access data they are authorized to access; and (ii) ensure that Customer Data cannot be read, copied, altered, or removed without authorization during processing, use, and after recording. The systems are designed to detect any inappropriate access. Nebul employs a centralized access management system to control personnel access to production servers and only provides access to a limited number of authorized personnel. Nebul's authentication and authorization systems utilize SSH certificates and security keys, and are designed to provide Nebul with secure and flexible access mechanisms. These mechanisms are designed to grant only approved access rights to site hosts, logs, data, and configuration information. Nebul requires the use of unique user IDs, strong passwords, two-factor authentication, and carefully monitored access lists to minimize the potential for unauthorized account use. The granting or modification of access rights is based on: the authorized personnel's job responsibilities; job duty requirements necessary to perform authorized tasks; and a need-to-know basis. The granting or modification of access rights must also be in accordance with Nebul's internal data access policies and training. Approvals are managed by workflow tools that maintain audit records of all changes. Access to systems is logged to create an audit trail for accountability. Where passwords are employed for authentication (e.g., login to workstations), password policies that follow at least industry-standard practices are implemented. These standards include restrictions on password reuse and sufficient password strength. For access to extremely sensitive information (e.g., credit card data), Nebul uses hardware tokens.

3. Data

(A) **Data Storage, Isolation, and Logging.** Nebul stores data in a multi-tenant environment on Nebul-owned servers. Subject to any Instructions to the contrary (e.g., in the form of a data location selection), Nebul replicates Customer Data between multiple geographically dispersed data centers. Nebul also logically isolates Customer Data. Customer will be given control over specific data-sharing policies. Those policies, in accordance with the functionality of the Services, will enable Customer to determine the product-sharing settings applicable to its End Users for specific purposes. Customer may choose to use logging functionality that Nebul makes available via the Services.

(B) **Decommissioned Disks and Disk Erase Policy.** Disks containing data may experience performance issues, errors, or hardware failure that lead them to be decommissioned ("Decommissioned Disk"). Every Decommissioned Disk is subject to a series of data destruction processes (the "Disk Erase Policy") before leaving Nebul's premises either for reuse or destruction. Decommissioned Disks are erased in a multi-step process and verified complete by at least two independent validators. The erase results are logged by the Decommissioned Disk's serial number for tracking. Finally, the erased Decommissioned Disk is released to inventory for reuse and redeployment. If, due to hardware failure, the Decommissioned Disk cannot be erased, it is securely stored until it can be destroyed. Each facility is audited regularly to monitor compliance with the Disk Erase Policy.

4. Personnel Security

Nebul personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. Nebul conducts reasonably appropriate background checks to the extent legally permissible and in accordance with applicable local labor law and statutory regulations.

Nebul personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, Nebul's confidentiality and privacy policies. Personnel are provided with security training. Personnel handling Customer Data are required to complete additional requirements appropriate to their role (e.g., certifications). Nebul's personnel will not process Customer Data without authorization.

5. Subprocessor Security

Before onboarding Subprocessors, Nebul conducts an audit of the security and privacy practices of Subprocessors to ensure Subprocessors provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Nebul has assessed the risks presented by the Subprocessor, then subject to the requirements described in Section 11.3 (Requirements for Subprocessor Engagement), the Subprocessor is required to enter into appropriate security, confidentiality, and privacy contract terms.

Schedule 4: Datacenters and Locations

Country, City	Datacenter Provider	Status – Planning
Netherlands, Amsterdam	Equinix	Online
Netherlands, Amsterdam	Digital Realty	Online
Netherlands, Hoofddorp	Eurofiber	Online
Germany, Hamburg	Atlas Edge	Planned December 2024
Belgium, Brussels	Atlas Edge	Planned June 2025

Schedule 5. Version Control

Version	Date	Status	Information
1.0	Sep 2023	Archive	Initial Addendum
1.1	June 2024	Current	Minor Updates