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 Personal Data is handled, stored, and secured. It is an integral part of our commitment to maintaining the highest standards of data privacy and security.

Version: V1.6 (April 2026)

Table of Contents

Schedules

DATA PROCESSING ADDENDUM (CUSTOMERS)

This Data Processing Addendum (including its appendices, the "Addendum") is incorporated into the Agreement (as defined in the Master Agreement) between Nebul and Customer. It applies where Nebul acts as a (sub)processor for 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 Personal Data. This Addendum will be effective on the Effective Date and will replace any terms previously applicable to the processing and security of Customer Personal Data. Capitalized terms used but not defined in this Addendum have the meaning given to them in the Master Agreement.

2. DURATION

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

3. ROLES; LEGAL COMPLIANCE

3.1 **Roles of Parties.** Nebul is a (sub)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 12 (Subprocessors);

B) Customer is responsible for forwarding any notice provided by Nebul under Section 7.1.1, 11.2.1 or 13.4 to the relevant controller; and

C) Customer may make available any information made available by Nebul to Customer under this Addendum to the relevant controller to comply with Applicable Laws.

4.2 **Compliance with Customer's Instructions.** Customer instructs Nebul to only process Customer Personal Data in accordance with the Agreement and Applicable Laws (collectively, the "Instructions"). Details of the Instructions are provided in Schedule 2.

4.3 Nebul will comply with the Instructions unless prohibited by Applicable Law. Nebul will notify Customer without undue delay if the Instructions breach Applicable Laws.

4.4 Nebul will refrain from processing Customer Personal data on any other ground than the Instructions unless legally required to do so by Applicable Laws. Nebul will inform Customer of this legal requirement unless prohibited to do so under Applicable Laws.

5. DATA DELETION

5.1 **Deletion by Customer.** Nebul will enable Customer to delete Customer Personal Data during the Term in a manner consistent with the functionality of the Services. If Customer uses the Services to delete any Customer Personal Data during the Term and that Customer Personal Data cannot be recovered by Customer, this use will constitute an Instruction to Nebul to delete the relevant Customer Personal Data from Nebul's systems. If Customer is not technically able to delete Customer Personal Data without Nebul's assistance, Customer may give an Instruction to Nebul to delete all remaining Customer Personal Data (including existing copies) from Nebul's systems. Nebul will comply with this Instruction as soon as reasonably practicable and within a maximum period of 180 days, unless Applicable Laws mandate longer retention of Customer Data.

5.2 **Return or Deletion When Term Ends.** Customer has the right have all remaining Customer Personal Data (including existing copies) deleted from Nebul's systems when the Agreement has ended unless Applicable Laws requires longer retention of Customer Personal Data, of which requirement Nebul will inform Customer. If Customer wishes to retain any Customer Personal Data after the end of the Agreement, Customer may give Nebul an Instruction to return Customer Personal Data instead.

5.3 **Deferred Deletion Instruction.** If an Instruction to delete Customer Personal Data pertains to one or more specific Service(s), and Nebul continues to process that Customer Personal Data in the context of other Services, the Addendum will continue to apply to such processing of Customer Personal Data. For clarity, this Addendum will continue to apply to the processing of Customer Personal Data for the provision of Services until Nebul has complied with Instructions to delete Customer Personal Data for all Services.

6. DATA SECURITY

6.1 **Nebul's Security Measures.** Nebul will implement and maintain appropriate technical, organizational, and physical measures to ensure the security of processing Customer Personal Data and to adequately protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access as described in Schedule 3 (the "Security Measures"). 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 Customer Personal Data.

6.2 **Access and Compliance.** Nebul will:

A) authorize its employees, contractors, and Subprocessors to access Customer Personal 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 Personal Data are under a contractual obligation of confidentiality.

6.3 **Additional Security Controls.** Nebul will make Additional Security Controls available to:

6.3.1 allow Customer to take further steps to secure Customer Personal Data; and

6.3.2 provide Customer with information about securing, accessing, and using Customer Personal Data.

7. PERSONAL DATA INCIDENTS

7.1.1 **Incident Notification.** Nebul will notify Customer without undue delay and no later than 72 hours after becoming aware of a Personal Data Incident and take reasonable steps to minimize harm and to secure Customer Personal Data.

7.1.2 **Details of** Personal **Data Incident.** Nebul's notification of a Personal Data Incident will describe: the nature of the Personal Data Incident including the Customer resources impacted; the measures Nebul has taken, or plans to take, to address the Personal Data Incident and mitigate its potential risk; the measures, if any, Nebul recommends that Customer takes to address the Personal 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 and further information will be provided without undue delay as it becomes available.

7.1.3 **No Assessment of Customer** Personal **Data by Nebul.** Except if and to the extent required under Applicable Laws, Nebul has no obligation to assess Customer Personal Data to identify of any Customer Personal Data is subject to specific legal requirements. It is Customer's responsibility to inform Nebul if this is the case. If such specific legal requirements apply, Nebul reserves the right to charge any additional costs to comply with such requirements to Customer.

7.1.4 **No Acknowledgement of Fault by Nebul.** Nebul's notification of or response to a Personal Data Incident under this Section 7 can under no circumstances be construed or qualify as an acknowledgement by Nebul of any fault or liability with respect to the Personal Data Incident.

7.1.5 **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 Personal Data Incident to the competent Supervisory Authority(ies). The responsibility of notifying the Personal Data Incident lies exclusively with the Customer or, if the Customer is a processor, the relevant controller.

8. CUSTOMER'S SECURITY RESPONSIBILITIES AND ASSESSMENT.

8.1 **Customer's Security Responsibilities.** Without prejudice to Nebul's obligations under Sections 6.1 and 7, and elsewhere in the Agreement, Customer is responsible for its use of the Services and its storage of any copies of Customer Personal 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 Personal 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 Personal Data as appropriate.

8.2 **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 Personal Data.

8.3 **Compliance Certifications.** Nebul will maintain at least the certificates for ISO 27001 ("Compliance Certifications") for the Audited Services to verify the continued effectiveness of the Security Measures. Nebul may add Compliance Certifications at any time. Nebul may replace the Compliance Certification with an equivalent or enhanced alternative.

9. AUDITS

9.1 **Reviews and Audits of Compliance.**

9.1.1 **Reviews of Compliance Certifications.** Nebul will make the information necessary to demonstrate compliance with the Addendum available for review upon request from the Customer including the Compliance Certifications.

9.1.2 **Customer's Audit Rights.**

Nebul will, if and to the extent required under Applicable Laws, allow Customer or an independent auditor appointed by Customer to conduct audits to verify Nebul's compliance with this Addendum in accordance with Section 9.1.3.

9.1.3 **Additional Business Terms for Reviews and Audits.**

A) Except in case of emergencies or following a Personal Data Incident, before conducting an audit, Customer must first contact Nebul's to request access to the Compliance Certifications. If the Compliance Certifications are not sufficient for the Customer, acting reasonably, to establish Nebul's compliance wit this Addendum, Customer may seek an audit.

B) Following a Customer request for an audit under Section 9.1.3 Nebul and Customer will discuss and agree in advance on the reasonable start date, scope, and duration of and security and confidentiality controls applicable to such audit.

C) Nebul may charge a fee (based on Nebul's reasonable costs) for any audit Customer performs or has performed. Nebul will provide Customer with further details of any applicable fee, and the basis of its calculation, in advance of any such request.

D) Customer will bear its own cost related to any audit, including any fees charged by any auditor appointed by Customer to execute such audit.

E) Nebul may object in writing to an auditor appointed by Customer to conduct any audit under Section 9.1.2 if the auditor is, in Nebul's reasonable opinion, not suitably qualified or independent, a competitor of Nebul, or otherwise manifestly unsuitable. If parties cannot reach agreement on the original auditor proposed by Customer and Nebul maintains its object, Customer will appoint another auditor or conduct the audit itself.

10. IMPACT ASSESSMENTS AND CONSULTATIONS

Taking into account the nature of the processing and the information available to Nebul, Nebul will assist Customer in ensuring compliance with its obligations relating to data protection impact assessments, risk assessments, prior consultations with the Competent Supervisory Authority or equivalent procedures under Applicable Laws.

11. ACCESS: DATA SUBJECT RIGHTS

11.1 **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 Personal Data, including via the deletion functionality provided by Nebul as described in Section 5.1, and to export Customer Personal Data. Customer is responsible for Customer Personal Data and for rectifying or deleting Customer Personal Data if required by Applicable Laws.

11.2 **Data Subject Requests.**

11.2.1 **Responsibility for Requests.** During the Term, if Nebul 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 request without written authorization from Customer or (if the Customer is a processor) from the relevant controller.

Vis-à-vis Nebul, Customer will be responsible for responding to any such request.

11.3 **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.

12. DATA PROCESSING LOCATIONS

12.1 **Data Storage and Processing Facilities.** Subject to Nebul's data location commitments all Customer Personal Data will remain within the EU. Customer Personal Data may be processed in any country where Nebul or its Subprocessors maintain facilities.

12.2 **Data Center Information.** The locations of Nebul's data centers are listed in Schedule 4.

13. SUBPROCESSORS

13.1 **Consent to Subprocessor Engagement.** Without prejudice to Section 13.3, Customer authorizes Nebul's engagement of Subprocessors. Customer agrees with the engagement of the Subprocessers listed in Schedule 4.

13.2 **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 Personal Data to the extent required to perform the obligations pursuant to and in accordance with the Agreement ; and

ii. the Subprocessor is bound to similar obligations as described in this Addendum; and

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

13.3 **Opportunity to Object to Subprocessors.**

A) When Nebul engages any Subprocessor not listed in Schedule 4, Nebul will, notify Customer at least 30 days' prior to the engagement of the name, location, and activities of this Subprocessor).

B) Customer may object to the engagement of a Subprocessor pursuant to Section 13.3 within 15 days after being notified. Parties will then in good faith discuss possible solutions to discuss alternative solutions. Customer may terminate the Agreement if parties cannot reach a solution. In that case all fees for the remainder of the Agreement will become immediately due and payable. Customer realizes that Nebul provides a one-to-many service and objecting to an individual Subprocessor will have significant impact on Nebul's ability to provide its services to its customer group as a whole. Therefore, Customer will only object to a proposed Subprocessor if it has serious and well-founded objections.

14. SAFE DATA PROTECTION; PROCESSING RECORDS

14.1 **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 Personal Data under the Agreement and can be contacted at security@nebul.com

14.2 **Nebul's Processing Records.** To the extent any Applicable Law requires Nebul to collect and maintain records of certain information relating to Nebul's processing of Customer Personal Data, Nebul will do so. Nebul may make any such information available to competent regulators, including a Supervisory Authority, if required by Applicable Law.

14.3 **Controller Requests.** If Nebul receives a request or instruction from a third party purporting to be a controller of Customer Personal Data, Nebul will refer that third party to Customer.

15. ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

15.1 **No Training on Customer Data.** Nebul explicitly acknowledges and agrees that it shall not use, log, store, or process any Customer Data (including Customer Personal Data), AI prompts inputted by the Customer or its End Users, or AI-generated responses resulting from such prompts, for the purpose of training, retraining, or fine-tuning any artificial intelligence or machine learning models.

15.2 **No Logging or Storage of AI Interactions.** Unless strictly necessary for the generation of a requested output or the provision of the Services as outlined in Schedule 2, Nebul shall not log, retain, or store any prompts, corresponding responses, or general Customer Data within its systems or those of its Subprocessors.

15.3 **Exceptions by Explicit Agreement.** The prohibitions established in Sections 15.1 and 15.2 shall apply universally; provided, however, that Nebul may log, store, or utilize such data for the aforementioned purposes solely if the Customer and Nebul have entered into an explicit, prior written agreement specifically outlining and authorizing the scope of such processing.

Schedule 1: Definitions

1. Definitions in 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.
- **"Audited Services"** means the 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 Agreement.
- **"Compliance Certifications"** has the meaning given in Section 6.4.
- **"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 Law.
- **"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.
- **"GDPR"** means, as applicable: (a) the EU GDPR; or (b) the UK GDPR.
- **"Instructions"** has the meaning given in Section 4.2).
- **"Personal 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 Personal Data on systems managed by or otherwise controlled by Nebul.
- **"Security Measures"** has the meaning given in Section 6.1.1.
- **"Sensitive Data"** means any: (i) Customer Personal Data that by itself or combined with other information can be used to infer special categories of personal data; (ii) financial records; and (iii) other sensitive or regulated information as defined under Applicable Privacy Law.
- **"Subprocessor"** means a third party authorized as another processor to process Customer Personal Data.
- **"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).
- **"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", "special categories of 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 Personal Data by Nebul in accordance with Section 5.1.

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.

Categories of Data
Customer Personal Data provided to Nebul via the Services, by (or at the direction of) Customer (or its End Users). Nebul has no control over what Customer Personal Data Customer provides to Nebul via the Services.

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

Nebul will implement and maintain the Security Measures described in this Schedule 3.

1. Data Center and Network Security

(A) Data Centers.

- **Infrastructure.** 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 Representatives 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 Personal Data. Nebul designs its systems to (i) only allow authorized persons to access data they are authorized to access; and (ii) ensure that Customer Personal 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 on Nebul-owned servers. Subject to any Instructions to the contrary (e.g., in the form of a data location selection). Nebul also logically isolates Customer Personal 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 Personal Data are required to complete additional requirements appropriate to their role (e.g., certifications). Nebul's personnel will not process Customer Personal 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 13.3, the Subprocessor is required to enter into appropriate security, confidentiality, and privacy contract terms.

Schedule 4: Sub processors and Locations of Data Centers

Table 1: Sub processors

Hosting Location	Legal name	Data processing activities
European Union	HubSpot, Inc	Customer Relations Management
European Union	Slack Technologies, LLC	Customer communications
European Union	Halo Service Solutions, Ltd	Customer support
European Union	Microsoft Corporation	Customer communications

Table 2: Datacenter providers & locations

Country, City	Datacenter Provider	Status – Planning
Netherlands, Amsterdam	Eurofiber	Online

Schedule 5. Version Control

Version	Date	Status	Information
1.0	Sep 2023	Archive	Initial Addendum
1.1	June 2024	Archive	Minor Updates
1.2	April 2025	Archive	Layout update (Nebul rebrand)
1.3	June 2025	Archive	Various Updates
1.4	June 2025	Archive	Various Updates
1.5	March 2026	Archive	Various Updates
1.6	June 2026	Current	Clause 15 Added