

Neat Data Protection Addendum for Customers

This Data Protection Addendum (“**DPA**”) is incorporated into and forms part of (and if applicable, amends the current version of) the Agreement (“**Agreement**”) between Neatframe Limited and its Affiliates (“**Neat**”), and the company receiving services from Neat (the “**Services**”) as set forth in the Agreement (“**Customer**”), each a “**Party**” and collectively the “**Parties**”. This DPA applies to and takes precedence over the Agreement, to the extent of any conflict. Capitalized terms not defined herein are defined as in applicable Data Protection Laws. Customer and Neat agree as follows:

1. **Definitions.** For purposes of this DPA:
 - 1.1 “**Affiliate**” means any entity that directly or indirectly controls, is controlled by, or is under common control with a party to this DPA, where “control” refers to direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.
 - a. “**Data Protection Laws**” means all applicable laws, regulations, and other legal or self-regulatory requirements in any jurisdiction relating to privacy, data protection, data security, breach notification, or the Processing of personal data, including without limitation, to the extent applicable, the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.*, including its regulations and the amendments made by the California Privacy Rights Act of 2020 (“**CCPA**”), privacy laws passed by other U.S. states (together with the CCPA, “**U.S. Privacy Laws**”), the General Data Protection Regulation, Regulation (EU) 2016/679 (“**GDPR**”), the United Kingdom Data Protection Act of 2018 (“**UK Privacy Act**”), and the Swiss Federal Act on Data Protection (“**FADP**”). For the avoidance of doubt, if Neat’s Processing activities involving Customer Personal Data are not within the scope of a given Data Protection Law, such law is not applicable for purposes of this DPA.
 - b. “**Data Subject**” means an identified or identifiable natural person to whom Customer Personal Data relates, and includes “consumer” as defined in Data Protection Laws.
 - c. “**EU SCCs**” means the Standard Contractual Clauses issued pursuant to Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, located at http://data.europa.eu/eli/dec_impl/2021/914/oj and completed as set forth herein.
 - d. “**Customer Personal Data**” includes “personal data,” “personal information,” “personally identifiable information,” and analogous terms, as defined by applicable Data Protection Laws, that Neat Processes to provide the Services under the Agreement.
 - e. “**Process**” and its cognates “Processing,” “Processed,” etc. mean any operation or set of operations performed on Customer Personal Data or on sets of Customer Personal Data, whether or not by automated means, such as collection, recording, organization, creating, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.
 - f. “**Security Breach**” means any accidental or unlawful acquisition, destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data. For the avoidance of doubt,

Security Breaches do not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, or other network attacks on firewalls or networked systems.

- g. **“Subprocessor”** means any third party that Neat engages to Process Customer Personal Data.
- h. **“UK Addendum”** means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner’s Office, located at <https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-DPA.pdf> and completed as set forth herein.
- i. The terms **“Business,” “Controller,” “Processor,”** and **“Service Provider”** are defined as in Data Protection Laws. **“Controller”** is deemed to also refer to **“Business,”** and **“Processor”** is deemed to also refer to **“Service Provider.”**

2. **Roles of the Parties; Scope and Purposes of Processing.**

- a. This DPA applies to all Customer Personal Data that Neat Processes on behalf of Customer to provide its Services under the Agreement.
- b. The Parties agree that to the extent that Customer is the Controller of Customer Personal Data, Neat is its Processor. To the extent that Customer is a Processor of Customer Personal Data, Neat is its Subprocessor.
- c. Neat will Process Customer Personal Data solely: (1) to fulfill its obligations to Customer under the Agreement, including this DPA; (2) on Customer’s behalf; and (3) in compliance with Data Protection Laws. Neat will:
 - i. not retain, use, or disclose Customer Personal Data outside of the direct business relationship between Customer and Neat;
 - ii. not “sell” or “share” any Customer Personal Data, as such terms are defined in applicable U.S. Privacy Laws, to any third party;
 - iii. not attempt to (1) re-identify any pseudonymized, anonymized, aggregate, or de-identified Customer Personal Data, or (2) link, identify, or otherwise create a relationship between Customer Personal Data and any other data, without Customer’s express written permission;
 - iv. comply with any applicable restrictions under U.S. Privacy Laws on combining Customer Personal Data with personal data that Neat receives from, or on behalf of, another person or persons, or that Neat collects from any interaction between it and any individual; and
 - v. not otherwise engage in any Processing of Customer Personal Data that is prohibited or not permitted by Processors or Service Providers under Data Protection Laws.
- d. Customer:

- i. Is solely responsible for complying with its obligations as a Controller under Data Protection Laws;
- ii. Represents and warrants that it has taken all legally required steps (including providing any notices and obtaining any consents) to ensure that its provision of Customer Personal Data to Neat for the Processing contemplated under the Agreement and this DPA is compliant with Data Protection Laws; and
- iii. Retains the right, upon reasonable notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of Customer Personal Data.

3. **Customer Personal Data Processing Requirements.** Neat will:

- a. Provide the same level of protection for the Customer Personal Data as is required under Data Protection Laws applicable to Customer, to the extent and as required by Data Protection Laws.
- b. Ensure that the persons it authorizes to Process the Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- c. Promptly notify Customer of (i) any third-party or Data Subject complaints regarding the Processing of Customer Personal Data; or (ii) any government or Data Subject requests for access to or information about Neat's Processing of Customer Personal Data on Customer's behalf (collectively, "**Customer Personal Data Request**"), unless prohibited by applicable law from making such notification. If Neat receives a Customer Personal Data Request, except to the extent that applicable law requires Neat to take any action with regard to the Customer Personal Data Request, Neat will await written instructions from Customer on how, if at all, to assist in responding.
- d. On Customer's reasonable request and at Customer's cost, provide reasonable assistance to Customer for:
 - i. The fulfilment of Customer's obligations to respond to verifiable requests by Data Subjects (or their lawful representatives) to exercise their rights under Data Protection Laws (such as rights to access or delete Customer Personal Data), to the extent that Customer is unable to fulfill these obligations on its own.
 - ii. Customer's (i) performance of a data protection impact assessment of Processing or proposed Processing of Customer Personal Data, when required by Data Protection Laws; and/or (ii) consultation with regulatory authorities in relation to the Processing or proposed Processing of Customer Personal Data, including complying with any applicable obligation upon Neat to consult with a regulatory authority in relation to Neat's Processing or proposed Processing of Customer Personal Data.
- e. Promptly notify Customer if Neat determines that it can no longer meet its obligations under this DPA or Data Protection Laws.

4. **Data Security.** Neat will implement appropriate administrative, technical, physical, and

organizational measures to protect Customer Personal Data, as set forth in Exhibit B.

5. **Security Breach.** Neat will notify Customer upon discovery of a Security Breach without undue delay, and in no event later than 72 hours. Neat will comply with the Security Breach-related obligations directly applicable to it under Data Protection Laws and will assist Customer in Customer's compliance with its Security Breach-related obligations, including without limitation by:
 - a. Taking steps to mitigate the effects of the Security Breach and reduce the risk to Data Subjects whose Customer Personal Data was involved; and
 - b. Providing Customer with the following information, to the extent known:
 - i. The nature of the Security Breach, including, where possible, how the Security Breach occurred, the categories and approximate number of Data Subjects concerned, and the categories and approximate number of Customer Personal Data records concerned;
 - ii. The likely consequences of the Security Breach; and
 - iii. Measures taken or proposed to be taken by Neat to address the Security Breach, including, where appropriate, measures to mitigate its possible adverse effects.
6. **Subprocessors.**
 - a. Customer acknowledges and agrees that Neat may use Subprocessors to Process Customer Personal Data in accordance with the provisions within this DPA and Data Protection Laws. Where Neat sub-contracts any of its rights or obligations concerning Customer Personal Data to a Subprocessor, Neat will: (i) take steps to select and retain Subprocessors that are capable of maintaining appropriate privacy and security measures to protect Customer Personal Data consistent with applicable Data Protection Laws; and (ii) enter into a written agreement with each Subprocessor requiring it to comply with obligations at least as restrictive as those imposed on Neat under this DPA.
 - b. Neat will maintain an up-to-date list of its Subprocessors. The initial list is available below in Exhibit C and Customer consents to Neat's use of the Subprocessors on this list. Neat will provide Customer with twenty (20) days' notice of any new Subprocessor added to the list prior to providing the new Subprocessor with Customer Personal Data or access thereto, except in exigent circumstances such as if the Services will be severely disrupted if Neat does not engage a new Subprocessor in fewer than 10 days. If Customer reasonably objects to a new Subprocessor within that 20-day period, Neat will not provide the Subprocessor with Customer Personal Data or access thereto, and the Parties will cooperate to resolve the objection. If the Parties cannot resolve the objection within a reasonable period of time, the Customer's sole and exclusive remedy is to terminate the Services or that portion of the Services involving the objected-to Subprocessor on written notice to Neat.
7. **Data Transfers.**
 - a. Neat may not engage in any cross-border Processing of Customer Personal Data, or transmit

(directly or indirectly) any Customer Personal Data to any country not deemed “adequate” by the relevant authorities, or any country outside of the country from which such Customer Personal Data was provided to Neat, unless it complies with Data Protection Laws. To the extent required by Data Protection Laws, Neat shall ensure that a lawful data transfer mechanism is in place prior to engaging in any onward transfers of Customer Personal Data.

- b. To the extent legally required, by entering into this DPA, Customer and Neat are deemed to have signed the EU SCCs, which form part of this DPA and (except as described in Sections 7(c) and (d) below) are deemed completed as follows:
 - i. Module 2 of the EU SCCs applies to transfers of Customer Personal Data from Customer (as a Controller) to Neat (as a Processor), and Module 3 of the EU SCCs applies to transfers of Customer Personal Data from Customer (as a Processor) to Neat (as a Subprocessor);
 - ii. Clause 7 (the optional docking clause) is included;
 - iii. Clause 9 (Use of sub-processors): The Parties select Option 2 (General written authorization). Section 6(b) of this DPA sets forth the initial list of Subprocessors and process for updating that list;
 - iv. Clause 11 (Redress): The optional language requiring that data subjects be permitted to lodge a complaint with an independent dispute resolution body is not included;
 - v. Clause 17 (Governing law): The Parties choose Option 1 (the law of an EU Member State that allows for third-Party beneficiary rights) and select the laws of Norway;
 - vi. Clause 18 (Choice of forum and jurisdiction): The Parties select the courts of Norway;
 - vii. Annexes I (List of Parties) and II (Technical and organizational measures) are completed as set forth in Exhibits A and B of this DPA, respectively; and
 - viii. Annex III (List of subprocessors) is not applicable because the Parties have chosen General Authorization under Clause 9, but Neat’s list of subprocessors is available at Exhibit C.
- c. To the extent legally required, by entering into this DPA, the Parties are deemed to be signing the UK Addendum, which forms part of this DPA and takes precedence over the rest of this DPA as set forth in the UK Addendum. The Tables within the UK Addendum are deemed completed as follows:
 - i. Table 1: The Parties’ details shall be the Parties and their affiliates to the extent any of them is involved in such transfer, and the Key Contact shall be the contacts set forth in the Agreement.
 - ii. Table 2: The Approved EU SCCs referenced in Table 2 shall be the EU SCCs as executed by the Parties and completed in Section 7(b) of this DPA.
 - iii. Table 3: Annexes I and II are set forth in Exhibits A and B below, respectively. Annex III

is inapplicable.

- iv. Table 4: Either Party may end this DPA as set out in Section 19 of the UK Addendum.
- d. For transfers of Customer Personal Data that are subject to the FADP, the EU SCCs form part of this DPA as set forth in Section 7(b) of this DPA, but with the following differences to the extent required by the FADP:
- i. References to the GDPR in the EU SCCs are to be understood as references to the FADP insofar as data transfers are subject exclusively to the FADP and not to the GDPR.
 - ii. The term “member state” in EU SCCs shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the EU SCCs.
 - iii. The relevant supervisory authority is the Swiss Federal Data Protection and Information Commissioner (for transfers subject to the FADP and not the GDPR), or both such Commissioner and the supervisory authority identified in the EU SCCs (where the FADP and GDPR apply, respectively).
8. **Audits.** Upon Customer’s reasonable written request, subject to reasonable confidentiality controls, and no more than once every twelve (12) calendar months, Neat will make available to Customer a copy of Neat’s most recent security and data protection reports, if applicable and available, to demonstrate compliance with this DPA and applicable Data Protection Laws (“Neat Reports”). To the extent that such Neat Reports do not provide reasonably sufficient information to demonstrate Neat’s compliance with this DPA and Data Protection Laws and on prompt notice from Customer, Neat will provide such additional information as Customer reasonably requests to demonstrate Neat’s compliance with this DPA and Data Protection Laws, provided that Customer will be subject to appropriate confidentiality requirements and Neat may redact information not related to its Processing of Customer Personal Data under the Agreement. Customer agrees that the procedures set forth in this Section 8 satisfy its audit rights, if any, under Data Protection Laws.
9. **Return or Destruction of Customer Personal Data.** Except to the extent required otherwise by applicable law, Neat will delete or return all Customer Personal Data within sixty (60) days of Customer’s written request. Notwithstanding the foregoing, Customer understands that Neat may retain Customer Personal Data as necessary for backup purposes, and Neat will delete such Customer Personal Data in accordance with its retention policies for archival media. To the extent not prohibited by applicable law, Neat will inform Customer if it is unable to delete Customer Personal Data for some other reason. Neat will abide by this DPA with respect to any Customer Personal Data for as long as such Customer Personal Data is retained.
10. **Survival.** The provisions of this DPA survive the termination or expiration of the Agreement for so long as Neat or its Subprocessors Process Customer Personal Data.

Exhibit A

ANNEX I TO THE EU SCCS

A. LIST OF PARTIES

Data exporter(s):

- Name: Customer, as identified in the Agreement.
- Address: As provided in the Agreement.
- Contact person's name, position, and contact details: As provided in the Agreement.
- Activities relevant to the data transferred under these Clauses: The data exporter receives the data importer's Services pursuant to their underlying Agreement.
- Role: Controller or Processor, as applicable

Data importer(s):

- Name: Neat.
- Address: As provided in the Agreement
- Contact person's name, position, and contact details: As provided in the Agreement.
- Activities relevant to the data transferred under these Clauses: The data importer provides Services to the data exporter pursuant to their underlying Agreement.
- Role: Processor or Subprocessor, as applicable

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred: Customer's workforce (employees, contractors, agents, etc.).

Categories of personal data transferred: Any Personal Data provided by Customer to Neat for purposes of Neat performing the Services pursuant to the Agreement.

Note: The media stream of a meeting is not stored in the device or in the remote database of Neat Pulse. While a remote administrator is accessing the device, the meeting participants would normally pause any confidential meeting discussion until the remote administrator disconnects. It is the responsibility of the Customer to codify such practice into their organization policy.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures: The Services are not intended to process Special Category Data as defined under GDPR Article 9.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis): Continuous for the duration of the Agreement.

Nature of the processing: To provide Services pursuant to the Agreement to Customer.

Purpose(s) of the data transfer and further processing: The purpose of the transfer to and further Processing of Customer Personal Data by Neat is for Neat to provide the Services to Customer, including:

- Service Provisioning of Users
- Device Provisioning
- Device Management
- Remote Infrastructure management of devices
- Associated support activities to troubleshoot issues and provide resolution.
- Communication Service that enables meetings to happen through the platform using third party providers.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: Customer Personal Data will be retained for the period of time necessary for Neat to provide the Services to Customer under the Agreement and/or in accordance with applicable legal requirements.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing: Same as above to the extent that Customer Personal Data is provided to Subprocessors for purposes of providing the Services.

C. COMPETENT SUPERVISORY AUTHORITY

To the extent legally permitted, the competent supervisory authority is the Norwegian data protection authority.

Exhibit B

NEAT DATA SECURITY MEASURES

Neat's Information Security Program includes specific security requirements for its personnel and all Subprocessors or agents who have access to Customer Personal Data ("Data Personnel"). Neat's security requirements cover the following areas:

1. General Security Measures and Standards

1.1. Security Program. The Processor shall maintain a comprehensive information security program, including appropriate technical and organizational measures, to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. The program shall be designed to ensure a level of security appropriate to the risks presented by the processing, in particular from a personal data breach.

1.2. Staff. The Processor shall ensure that all personnel who have access to Customer Personal Data are informed of the confidential nature of such data and have been trained on the proper handling of personal data. The Processor shall ensure that such personnel are subject to confidentiality obligations.

1.3. Policies and Procedures. The Processor shall maintain and enforce written security policies and procedures that cover its processing of Customer Personal Data. The Processor shall review and update these policies and procedures at reasonable intervals to ensure their continued effectiveness.

1.4. Security Incidents. The Processor shall have a plan for responding to security incidents and personal data breaches. This plan shall include procedures for detection, analysis, containment, and notification.

2. Physical and Environmental Security

2.1. Access Controls. The Processor shall implement and maintain physical access controls to its facilities where Customer Personal Data is processed or stored. These controls shall prevent unauthorized access and protect against environmental threats such as fire, water damage, and theft.

2.2. Visitor Management. The Processor shall maintain a visitor management policy to ensure that all visitors to its facilities are properly identified, logged, and supervised.

2.3. Media and Equipment Disposal. The Processor shall ensure the secure disposal of all media and equipment that contains Customer Personal Data, in a manner that prevents unauthorized access.

3. Network and Systems Security

3.1. Network Security. The Processor shall employ network security controls, including firewalls and intrusion detection/prevention systems, to protect its network from unauthorized access.

3.2. Access Management. The Processor shall implement and maintain a formal access management policy that ensures access to Customer Personal Data is granted on a "need-to-know" and "least privilege" basis. This includes:

- Unique user IDs for all personnel with access to the data.

- Strong password policies or multi-factor authentication.
- Regular review and revocation of access rights.

3.3. Encryption. The Processor shall use industry-standard encryption technologies to protect Customer Personal Data:

- **Encryption in transit:** All data transmitted over public networks shall be encrypted.
- **Encryption at rest:** Data stored on disks, databases, or other storage media shall be protected by encryption, where feasible and appropriate.

3.4. Vulnerability Management. The Processor shall maintain a vulnerability management program, including a process for identifying, assessing, and remediating security vulnerabilities in its systems. This program shall include regular scanning and patching.

4. Application and Data Security

4.1. Secure Development. The Processor shall follow secure coding practices and conduct security testing of its applications to ensure they are free from common vulnerabilities.

4.2. Logging and Monitoring. The Processor shall maintain a logging and monitoring system to record user access and activities related to Customer Personal Data. These logs shall be regularly reviewed for suspicious activities.

4.3. Data Backup and Recovery. The Processor shall maintain a backup and recovery plan to ensure the availability of Customer Personal Data in the event of an incident or disaster. Backups shall be tested periodically to ensure their integrity.

Exhibit C: Neat List of Approved Subprocessors

The following subprocessors have been vetted and may be involved in aspects of processing Customer Personal Data in the course of assisting Neat in its provision of Services to Customer.

Subprocessors	Purpose of Processing Activity	Registered Business Address	Location of Processing	Link to Privacy / Security Policy
Google LLC	GCP Public Cloud Hosting Provider	1600 Amphitheatre Parkway Mountain View, CA 94043 United States	United States Europe	Privacy Policy
Mailjet	Email Delivery Service	Mailgun Technologies, Inc., 112 E Pecan St #1135, San Antonio, TX 78205, US	United States	DPA - Email Marketing - SMTP services Mailjet Mailjet Personal Data Protection and Privacy Policy Mailjet
Microsoft Corporation	Azure Public Cloud Hosting Provider	920 Fourth Avenue, Suite 2900, Seattle, Washington 95104, US	West Europe (Netherlands) West US 2 (Washington)	Licensing Documents (microsoft.com) Microsoft Privacy Statement – Microsoft privacy
Pendo	Usage Analytics	301 Hillsborough St. Suite 1900 Raleigh, NC 27603, US	United States	Data Privacy and Security Pendo.io Data Processing Addendum Pendo.io
Zendesk	Customer Support	1019 Market St., San Francisco, CA 94103, US	United States	Zendesk Privacy Policy Zendesk Trust Center