DATA PROCESSING ADDENDUM

This Data Processing Addendum ("Addendum") including its Annexes and Appendices forms part of the written electronic agreement, and is made by and between:

1. **Customer:**

Name	
Address	
GDPR Role (Controller / Processor)	
Contact person's name, position, and contact details:	

2. **Vendor:**

Name	Neatframe Limited (Companies House Identifier: 11802958)
Address	Cannon Green, 27 Bush Lane, London, United Kingdom, EC4R 0AA
GDPR Role	Processor
Contact person's name, position, and contact details:	Steve Odegaard, Chief Information Security Officer, neat.privacy@neat.no

WHEREAS, both Customer and Vendor may be collectively referred to as the Parties;

WHEREAS, the Parties have agreed that it will be necessary for the Vendor to process certain personal data on behalf of the Customer; and

WHEREAS, in light of this processing, the Parties have agreed to the terms of this Addendum to address the compliance obligations imposed upon them to the Data Protection Law listed under Sec 1.2 below as applicable;

NOW THEREFORE, the Parties hereby agree as follows.

1 SUBJECT MATTER OF THIS DATA PROCESSING ADDENDUM

1.1 This Data Processing Addendum applies exclusively to the processing of personal data that is subject to Data Protection Law in the scope of the Addendum between the Parties for the Neat Pulse ("Services").

1.2 The term “**Data Protection Law**” shall mean all Applicable Laws relating to data protection, the processing of personal data and privacy including,

1.2.1 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 (hereinafter “GDPR”);

1.2.2 Regulation EU 2018/1725 of the European Parliament and of the Council of 23 October 2018

1.2.3 UK GDPR (General data protection regulation – Keeling schedule) and United Kingdom’s Data Protection Act 2018

1.2.4 The Brazilian General Data Protection Law or “Lei Geral de Proteção de Dados Pessoais” (“LGPD”) as amended by Law No.13,853/2019.

1.2.5 the Swiss Federal Act on Data Protection ("Swiss FADP").

1.2.6 Applicable US Federal or State Legislations related to cyber security, data protection and privacy that is applicable to this engagement to the extent it is applicable to Customer, which includes, but not limited to:

a) CCPA - California Consumer Privacy Act of 2018 (Cal. Civ. Code §§ 1798.100 to 1798.199) as amended by California Privacy Rights Act of 2020 (CPRA) and the California Consumer Privacy Act Regulations (Cal. Code Regs. tit. 11, §§ 999.300 to 999.337) as amended or superseded from time to time (the “CCPA”), and any related regulations or guidance provided by the California Attorney General.

b) The Health Insurance Portability and Accountability Act of 1996 (HIPAA).

c) The Colorado Privacy Act of 2021

d) The Virginia Consumer Data Protection Act of 2021

e) The Utah Consumer Privacy Act of 2022

1.2.7 Canada’s Federal legislation, The Personal Information Protection and Electronic Documents Act (PIPEDA) and other provincial legislations such as but not limited to 'PIPA Alberta', 'PIPA BC' and 'Quebec Privacy Act'.

1.2.8 Any national data protection law implemented by an EU/EEA member to supplement the GDPR, such as but not limited to Norwegian Personal Data Act, Germany’s Bundesdatenschutzgesetz (BDSG), Denmark’s Data Protection Act, etc. as relevant to the jurisdiction and the processing of personal or sensitive information.

1.2.9 Any equivalent applicable legislation in any jurisdiction in which the Customer is established to the extent applicable to the Customer and as communicated to the Vendor.

1.2.10 The above-mentioned legislations as amended, consolidated, restated or re-enacted from time to time.

1.3 Terms such as “Processing”, “Personal Data”, “Data Controller” and “Processor” shall have the meaning ascribed to them in the EU Data Protection Law.

1.4 The Term “Service Agreement” may refer to the Terms and Conditions present in Sales Orders placed with your Neat Partner of choice or the Neat Pulse Agreement available at https://neat.no/neat-pulse-terms-and-conditions/.

1.5 Insofar as the Vendor will be processing Personal Data subject to Data Protection Law on behalf of the Customer in the course of the performance of the Service Agreement with the Customer the terms of this Data Processing Addendum shall apply. An overview of the categories of Personal Data, the types of Data Subjects, and purposes for which the Personal Data are being processed is provided in Annex 2.

1.6 “Standard Contractual Clauses" means: (i) where the EU GDPR applies, the standard contractual clauses annexed to the European Commission's Implementing Decision 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 (the "EU SCCs"); and (ii) where the UK GDPR applies, the “International Data Transfer Addendum to the EU Commission Standard Contractual Clauses VERSION B1.0” issued by the Information Commissioner’s Office under s.119A (1) of the United Kingdom Data Protection Act 2018 in respect of the transfer of such Personal Data ("UK SCCs") and (iii) where the Swiss FADP applies, the applicable standard data protection clauses issued, approved or otherwise recognized by the Swiss Federal Data Protection and Information Commissioner ("FDPIC") (the "Swiss SCCs").

2 LEGAL BASIS OF PROCESSING

2.1 The Customer will determine the scope, purposes, and manner by which the Personal Data may be accessed or processed by the Vendor. The Vendor will process the Personal Data only as set forth in Customer’s written instructions.

2.2 The Vendor will only process the Personal Data on documented instructions of the Customer (including with regard to transfers of personal data to a third country or an international organization, unless required to do by Union or Member State law to which the Vendor is subject) in such manner as, and to the extent that, this is appropriate for the provision of the Services, except as required to comply with a legal obligation to which the Vendor is subject. In such a case, the Vendor shall inform the Customer of that legal obligation before processing, unless that law explicitly prohibits the furnishing of such information to the Customer. The Vendor shall never process the Personal Data in a manner inconsistent with the Customer’s documented instructions. The Vendor shall immediately inform the Customer if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.

2.3 The Parties have entered into a Service Agreement in order to benefit from the expertise of the Vendor in securing and processing the Personal Data for the purposes set out in Annex 2. The Vendor shall be allowed to exercise its own discretion in the selection and use of such means as it considers necessary to pursue those purposes, subject to the requirements of this Data Processing Addendum.

2.4 Customer warrants that it has all necessary rights to provide the Personal Data to Vendor for the Processing to be performed in relation to the Services. To the extent required by Applicable Data Protection Law, Customer is responsible for ensuring that any necessary data subject consents to this Processing are obtained, and for ensuring that a record of such consents is maintained. Should such a consent be revoked by the data subject, Customer is responsible for communicating the fact of such revocation to the Vendor, and Vendor remains responsible for implementing any Customer instruction with respect to the further processing of that Personal Data.

3 CONFIDENTIALITY

3.1 Without prejudice to any existing contractual arrangements between the Parties, the Vendor shall treat all Personal Data as strictly confidential and it shall inform all its employees, agents and/or approved sub-processors engaged in processing the Personal Data of the confidential nature of the Personal Data. The Vendor shall ensure that all such persons or parties have signed an appropriate confidentiality agreement, are otherwise bound to a duty of confidentiality, or are under an appropriate statutory obligation of confidentiality.

4 SECURITY

4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, without prejudice to any other security standards agreed upon by the Parties, the Customer and Vendor shall implement appropriate technical and organisational measures to ensure a level of security of the processing of Personal Data appropriate to the risk. These measures shall include as appropriate:

4.1.1 measures to ensure that the Personal Data can be accessed only by authorized personnel for the purposes set forth in Annex 2 of this Data Processing Addendum;

4.1.2 In assessing the appropriate level of security account shall be taken in particular of all the risks that are presented by processing, for example from accidental or unlawful destruction, loss, or alteration, unauthorized or unlawful storage, processing, access or disclosure of Personal Data;

4.1.3 the pseudonymisation and encryption of personal data;

4.1.4 the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

4.1.5 the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

4.1.6 a process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing of Personal Data;

4.1.7 measures to identify vulnerabilities regarding the processing of Personal Data in systems used to provide services to the Customer; and

4.1.8 the measures agreed upon by the Parties in Annex 3.

4.2 The Vendor shall at all times have in place an appropriate written security policy with respect to the processing of Personal Data, outlining in any case the measures set forth in Section 4.1.

4.3 At the request of the Customer, the Vendor, shall demonstrate the measures it has taken pursuant to this Section 4 shall allow the Customer to audit and test such measures. The Customer shall be entitled on giving at least 14 days’ notice to the Vendor to carry out, or have carried out by a third party who has entered into a confidentiality agreement with the Vendor, audits of the Vendor´s premises and operations as these relate to the Personal Data. The Vendor shall cooperate with such audits carried out by or on behalf of the Customer and shall grant the Customer´s auditors reasonable access to any premises and devices involved with the Processing of the Personal Data. The Vendor shall provide the Customer and/or the Customer´s auditors with access to any information relating to the Processing of the Personal Data as may be reasonably required by the Customer to ascertain the Vendor´s compliance with this Data Processing Addendum.

5 IMPROVEMENTS TO SECURITY

5.1 The Parties acknowledge that security requirements are constantly changing and that effective security requires frequent evaluation and regular improvements of outdated security measures. The Vendor will therefore evaluate the measures as implemented in accordance with Section 4 on an on-going basis and will tighten, supplement and improve these measures in order to maintain compliance with the requirements set out in Section 4. The Parties will negotiate in good faith the cost, if any, to implement material changes required by specific updated security requirements set forth in applicable data protection law or by data protection authorities of competent jurisdiction.

5.2 Where an amendment to the Service Agreement is necessary in order to execute a Customer instruction to the Vendor to improve security measures as may be required by changes in applicable data protection law from time to time, the Parties shall negotiate an amendment to the Service Agreement in good faith.

6 DATA TRANSFERS

6.1 If the storage and/or processing of Personal Data involves transfers of Personal Data out of the EEA, then the Vendor shall be obliged to meet at least one of the following conditions:

6.1.1 Ensure the destination meets the European Commission's level of adequacy per Article 45 of the Regulation (GDPR); or

6.1.2 Ensure the destination employs an approved European Commission legal mechanism; or

6.1.3 Ensure the destination has entered into an acceptable EU Model Contract Clause specifying the appropriate importer and exporter designations, requirements and safeguards; or

6.1.4 Employs an alternative solution that meets the requirements of the European commission such as Binding Corporate Rules per Article 63 of the Regulation.

6.2 The Vendor shall immediately notify the Customer of any planned, permanent or temporary transfers of Personal Data to a country outside of the European Economic Area without an adequate level of protection and shall only perform such transfer after obtaining authorisation from the Customer, which may be refused at its own discretion.

6.3 Annex 4 provides a list of transfers for which the Customer grants its consent upon the conclusion of this Data Processing Addendum.

6.4 To the extent that the Customer or the Vendor are relying on a specific statutory mechanism to normalize international data transfers that is subsequently modified, revoked, or held in a court of competent jurisdiction to be invalid, the Customer and the Vendor agree to cooperate in good faith to promptly terminate the transfer or to pursue a suitable alternate mechanism that can lawfully support the transfer.

6.5 This DPA incorporates the Standard Contractual Clauses by reference. By executing this DPA, the Customer enters this DPA (including the Standard Contractual Clauses referenced herein, if applicable) on behalf of itself and any Affiliates authorized to use the Services under the Agreement and who have not entered into a separate contractual arrangement with the Vendor.

6.6 It is not the intention of either Party to contradict or restrict any of the provisions set forth in the Standard Contractual Clauses and, accordingly, if and to the extent the Standard Contractual Clauses conflict with any provision of the Agreement (including this DPA) the Standard Contractual Clauses shall prevail to the extent of such conflict.

6.7 **Transfers outside EEA:** In relation to EU data protected by the EU GDPR, the EU Standard Contractual Clauses apply to such transfers, completed as follows.

6.7.1 MODULE ONE: Transfer controller to controller of the EU SCCs shall apply when both the Customer and Vendor act as a Controller.

6.7.2 MODULE TWO: Transfer controller to processor of the EU SCCs shall apply when the Customer is a Controller and Vendor is a Processor.

6.7.3 MODULE THREE: Transfer processor to processor of the EU SCCs shall apply when both the Customer and Vendor act as a Processor.

6.7.4 Annex I of the EU SCCs shall be deemed completed with the information set out in Annex 1,2, 4 of this DPA.

6.7.5 Annex II of the EU SCCs shall be deemed completed with the information set out in Annex 3 of this DPA.

6.7.6 Clause 7 – Docking clause (optional) will apply.

6.7.7 Clause 9 (a) OPTION 2 – General written authorization for subprocessors will apply and the time period to object will be Thirty days.

6.7.8 Clause 11(a) – OPTION to use independent resolution body shall not apply.

6.7.9 Clause 17, Option 2 will apply, and the parties agree that this shall be the law of Norway.

6.7.10 Clause 18(b), disputes shall be resolved before the courts of Norway.

6.8 **Transfers outside Switzerland:** In relation to Personal Data that is protected by the Swiss FADP, the EU SCCs will apply in accordance with Section 6.6 with the following modifications:

6.8.1 any references in the EU SCCs to "Directive 95/46/EC" or "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss FADP;

6.8.2 references to "EU", "Union", "Member State" and "Member State law" shall be interpreted as references to Switzerland and Swiss law, as the case may be; and

6.8.3 references to the "competent supervisory authority" and "competent courts" shall be interpreted as references to the FDPIC and competent courts in Switzerland, unless the EU SCCs as implemented above cannot be used to lawfully transfer such Personal Data in compliance with the Swiss FADP, in which event the Swiss SCCS shall instead be incorporated by reference and form an integral part of this Addendum and shall apply to such transfers. Where this is the case, the relevant Annexes of the Swiss SCCs shall be populated using the information contained in Annex 1,2,3,4 to this Addendum (as applicable).

6.9 **Transfers outside UK:** In relation to Personal Data that is protected by the UK GDPR, the UK SCCs shall apply, completed as follows:

6.9.1 The EU Standard Contractual Clauses shall be deemed amended as specified by the UK SCCs;

6.9.2 Reference to Table 1 shall be satisfied by the information in Annex 1;

6.9.3 Table 2, The version of the Approved EU SCCs shall be the EU SCCs identified in Sec 1.6 and completed as set out in Section 6.7 above;

6.9.4 Reference to Table 3 shall be se satisfied by the information in Annexes 1, 2, 3 and 4;

6.9.5 Table 4, Importer and Exporter shall have the rights outlined in Section 19 of UK SCCs.

7 INFORMATION OBLIGATIONS AND INCIDENT MANAGEMENT

7.1 When the Vendor becomes aware of an incident that impacts the Processing of the Personal Data that is the subject of the Service Agreement, it shall promptly notify the Customer about the incident, shall at all times cooperate with the Customer, and shall follow the Customer's instructions with regard to such incidents, in order to enable the Customer to perform a thorough investigation into the incident, to formulate a correct response, and to take suitable further steps in respect of the incident.

7.2 The term "incident" used in Section 7.1 shall be understood to mean in any case:

7.2.1 a complaint or a request with respect to the exercise of a data subject's rights under EU Data Protection Law;

7.2.2 an investigation into or seizure of the Personal Data by government officials, or a specific indication that such an investigation or seizure is imminent;

7.2.3 any unauthorized or accidental access, processing, deletion, loss or any form of unlawful processing of the Personal Data;

7.2.4 any breach of the security and/or confidentiality as set out in Sections 3 and 4 of this Data Processing Addendum leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, the Personal Data, or any indication of such breach having taken place or being about to take place;

7.2.5 where, in the opinion of the Vendor, implementing an instruction received from the Customer would violate applicable laws to which the Customer or the Vendor are subject.

7.3 The Vendor shall at all times have in place written procedures which enable it to promptly respond to the Customer about an incident. Where the incident is reasonably likely to require a data breach notification by the Customer under applicable EU Data Protection Law, the Vendor shall implement its written procedures in such a way that it is in a position to notify the Customer without undue delay of having become aware of such an incident.

7.4 Any notifications made to the Customer pursuant to this Section 7 shall be addressed to the employee of the Customer whose contact details are provided in Annex 1 of this Data Processing Addendum, and shall contain:

7.4.1 a description of the nature of the incident, including where possible the categories and approximate number of data subjects concerned and the categories and approximate number of Personal Data records concerned;

7.4.2 the name and contact details of the Vendor's data protection officer or another contact point where more information can be obtained;

7.4.3 a description of the likely consequences of the incident; and

7.4.4 a description of the measures taken or proposed to be taken by the Vendor to address the incident including, where appropriate, measures to mitigate its possible adverse effects.

8 CONTRACTING WITH SUB-PROCESSORS

8.1 The Customer authorises the Vendor to engage sub-processors for the service-related activities specified as described in Annex 2. Vendor shall not add or replace any such sub-processors listed in Annex 4 without giving the Customer an opportunity to object to such changes.

8.2 The Vendor shall not engage in any future subcontracting of its Service-related activities related to the processing of the Personal Data or requiring Personal Data to be processed by any third party without the prior written authorisation of the Customer.

8.3 Notwithstanding any authorisations by the Customer within the meaning of the preceding paragraphs, the Vendor shall remain fully liable vis-à-vis the Customer for the performance of any such subprocessor that fails to fulfil its data protection obligations.

8.4 The consent of the Customer pursuant to paragraphs 8.1 and 8.2 shall not alter the fact that consent is required under Section 6 for the engagement of sub-processors in a country outside the European Economic Area without a suitable level of protection.

8.5 The Vendor shall ensure that the sub-processor is bound by the same data protection obligations of the Vendor under this Data Processing Addendum, shall supervise compliance thereof, and must in particular impose on its sub-processors the obligation to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of EU Data Protection Law.

8.6 The Customer may request that the Vendor audit a Third Party Subprocessor or provide confirmation that such an audit has occurred (or, where available, obtain or assist customer in obtaining a third-party audit report concerning the Third Party Subprocessor's operations) to ensure compliance with its obligations imposed by the Vendor in conformity with this Addendum.

8.7 The Vendor shall not engage any Subprocessors located outside of European Economic Area without employing an acceptable instrument for cross-border data transfers such as Standard Contractual Clauses, Binding Corporate Rules or an Article 49 derogation.

9 RETURNING OR DESTRUCTION OF PERSONAL DATA

9.1 Upon termination of this Data Processing Addendum, upon the Customer's written request, or upon fulfillment of all purposes agreed in the context of the Services whereby no further processing is required, the Vendor shall, at the discretion of the Customer, either delete, destroy or return all Personal Data to the Customer and destroy or return any existing copies.

9.2 The Vendor shall notify all third parties supporting its own processing of the Personal Data of the termination of the Data Processing Addendum and shall ensure that all such third parties shall either destroy the Personal Data or return the Personal Data to the Customer, at the discretion of the Customer.

10 ASSISTANCE TO CUSTOMER

10.1 The Vendor shall assist the Customer by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising the data subject's rights under the GDPR.

10.2 The Vendor shall assist the Customer in ensuring compliance with the obligations pursuant to Section 4 (Security) and prior consultations with supervisory authorities required under Article 36 of the GDPR taking into account the nature of processing and the information available to the Vendor.

10.3 The Vendor shall make available to the Customer all information necessary to demonstrate compliance with the Vendor's obligations and allow for and contribute to audits, including inspections, conducted by the Customer or another auditor mandated by the Customer.

10.4 The Vendor shall assist the Customer in carrying out data protection impact assessments when requested.

10.5 The Customer shall bear any costs accrued by the Vendor related to any assistance in sections 10.1 – 10.4, unless otherwise agreed.

11 LIABILITY AND INDEMNITY

11.1 Notwithstanding any other provisions in this Addendum, each Party's liability towards the other for indirect, consequential, or punitive damages shall be limited, except as expressly provided in this Addendum. However, nothing in this Addendum shall limit or exclude either Party's liability for breaches of Data Protection Laws, including obligations under GDPR, or for any other liability which cannot be excluded or limited under applicable law. Both Parties commit to maintaining compliance with all relevant data protection regulations and to cooperate in good faith to address any data protection issues that arise in the course of providing and using the services.

12 DURATION AND TERMINATION

12.1 This Data Processing Addendum shall come into effect as of the date of this contract execution as noted in the signature block.

12.2 Termination or expiration of this Data Processing Addendum shall not discharge the Vendor from its confidentiality obligations pursuant to Section 3.

12.3 The Vendor shall process Personal Data until the date of termination of the Service Agreement, unless instructed otherwise by the Customer, or until such data is returned or destroyed on instruction of the Customer.

13 TERMS APPLICABLE TO US PERSONAL DATA

13.0 Terms defined in the CCPA, including personal information and business purposes, carry the same meaning in this Addendum. These terms apply with respect to other US personal data, governed by respective US privacy laws, only to the extent to which the law mandates.

13.0.1 “Contracted Business Purposes” means the services described in the Agreement and Appendices and Addendums for which the Service Provider receives or accesses personal information.

13.0.2 "Authorized Persons" means the persons or categories of persons that the Data Exporter authorizes to provide the Service Provider with personal information processing instructions, as identified in the appendices.

13.0.3 “Vendor” is referred to as “Service Provider” in line with CCPA terminology in this section.

13.0.4 Other definitions used in this Addendum shall have the meaning of the defined terms from Cal. Civ. Code § 1798.140; Cal. Code Regs. tit. 11, §999.301.

Service Provider ‘s Obligations

13.1 Service Provider will only collect, use, retain, or disclose personal information for the Contracted Business Purposes for which the Customer provides or permits personal information access in accordance with the Customer's written instructions from Authorized Persons.

13.2 Service Provider will not collect, use, retain, disclose, sell, or otherwise make personal information available for Service Provider's own commercial purposes or in a way that does not comply with the CCPA. If a law requires the Service Provider to disclose personal information for a purpose unrelated to the Contracted Business Purpose, the Service Provider must first inform the Customer of the legal requirement and give the Customer an opportunity to object or challenge the requirement, unless the law prohibits such notice.

13.3 Service Provider will process personal information only as necessary to perform the Services, and will not, under any circumstances, collect, combine, share, use, retain, access, share, transfer, or otherwise process personal information for any purpose not related to providing such Services. Service Provider will refrain from taking any action that would cause any transfers of Customer Data to or from Lever to qualify as “selling personal information” under CCPA.

13.4 Service Provider must promptly comply with any Customer request or instruction from Authorized Persons requiring the Service Provider to provide, amend, transfer, or delete the personal information, or to stop, mitigate, or remedy any unauthorized processing.

13.5 If the Contracted Business Purposes require the collection of personal information from individuals on the Customer's behalf, Service Provider will always provide a CCPA-compliant notice at collection that the Customer specifically pre-approves in writing. Service Provider will not modify or alter the notice in any way without the Customer's prior written consent.

13.6 Service Provider will use commercially reasonable security procedures that are reasonably designed to maintain an industry-standard level of security, prevent unauthorized access to and/or disclosure of Customer Data. An outline of minimum-security standards can be found at Annex 3 of this DPA. Upon request by Customer, Service Provider shall provide information security compliance documentation and allow other measures including ongoing manual reviews and automated scans and regular assessments, audits or other technical and operational testing at least once every 12 months.

13.7 Service Provider will retain Personal Data only for as long as the Customer deems it necessary for the permitted purpose, or as required by applicable laws. At the termination of this addendum, or upon Customer’s written request, Service Provider will either destroy or return Personal Data, unless legal obligations require storage of such Personal Data.

Customer’s CCPA Obligations

13.8 Service Provider will reasonably cooperate and assist Customer with meeting the Customer’s CCPA compliance obligations (which address obligations with regard to security, breach notifications, data risk assessments, and prior consultation) and responding to CCPA-related inquiries, including responding to verifiable consumer requests, taking into account the nature of the Service Provider's processing and the information available to the Service Provider.

13.9 Service Provider must notify the Customer immediately if it receives any complaint, notice, or communication that directly or indirectly relates either party's compliance with the CCPA. Specifically, the Service Provider must notify the Customer within ten (10) working days if it receives a verifiable consumer request under the CCPA.

Subcontracting

13.10 Service Provider may employ subcontractors to provide the Contracted Business Services, provided always that such engagement shall be subject to a written contract binding with each such Sub-Service Provider to terms no less onerous than those contained within this addendum. Annex 4 of this DPA provides a list of Sub-service providers. Any subcontractor used must qualify as a service provider under the CCPA and Service Provider cannot make any disclosures to the subcontractor that the CCPA would treat as a sale.

13.11 Upon Customer’s written request, for each subcontractor used, Service Provider will give Customer an up-to-date list disclosing.

13.11.1 The subcontractor's name, address, and contact information.

13.11.2 The type of services provided by the subcontractor.

13.11.3 The personal information categories disclosed to the subcontractor in the preceding 12 months.

13.12 Service Provider remains fully liable to the Customer for the subcontractor's performance of its agreement obligations.

13.13 Upon the Customer's written request, Service Provider will provide the Customer with the privacy and security assurances relating to subcontractor's compliance with its personal information obligations.

Warranties

13.14 Both parties will comply with all applicable requirements of the CCPA when collecting, using, retaining, or disclosing personal information.

13.15 Service Provider certifies that it understands this Addendum's and the CCPA's restrictions and prohibitions on selling personal information and retaining, using, or disclosing personal information outside of the parties' direct business relationship, and it will comply with them.

13.16 Service Provider warrants that it has no reason to believe any CCPA requirements or restrictions prevent it from providing any of the Contracted Business Purposes or otherwise performing under this Agreement. Service Provider must promptly notify the Customer of any changes to the CCPA's requirements that may adversely affect its performance under the Agreement. If Customer has reasonable cause to suspect that Service Provider is not providing the services in a manner consistent with CPRA and allowing unauthorized use of Personal Data, the Customer may (i) submit an inquiry to privacy@pexip.com, (ii) cease use of their license until they are able to confirm the compliance, or (iii) with evidence of non-compliance of CPRA terminate the Agreement between the parties.

14 MISCELLANEOUS

14.1 In the event of any inconsistency between the provisions of this Data Processing Addendum and the provisions of the Service Agreement, the provisions of this Data Processing Addendum shall prevail.

14.2 This Data Processing Addendum is governed by the laws noted in the Service Agreement.

NOW THEREFORE, the Parties hereby execute this addendum.

Signed for and on behalf of the Customer	Signed for and on behalf of the Customer (Optional block for second signatory):
Name:	Name:
Title:	Title:
Date:	Date:
Signature	Signature

Signed for and on behalf of the Vendor
Name:
Title:
Date:
Signature

Annex 1: List of Parties and Competent Supervisory Authority

LIST OF PARTIES

Refer page1 of DPA for list of Parties along with their roles.

Activities relevant to the data transferred under these Clauses: Refer Sec 1.1 of this DPA.

COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority, in accordance with Clause 13 of the EU SCCs, must be

(i) the supervisory authority applicable to the data exporter in its EEA country of establishment or,

(ii) where the data exporter is not established in the EEA, the supervisory authority applicable in the EEA country where the data exporter's EU representative has been appointed pursuant to Article 27(1) of the GDPR, or

(iii) where the data exporter is not obliged to appoint a representative, the supervisory authority applicable to the EEA country where the data subjects relevant to the transfer are located.

(iv) with respect to Customer Data regulated by the UK GDPR, the competent supervisory authority is the Information Commissioners Office (the "ICO").

(v) with respect to Customer Data regulated by the Brazil General Data Protection Law or LGPD, the competent supervisory authority is the ANPD - "Autoridade Nacional de Proteção de Dados''.

(vi) with respect to Customer Data to which the Swiss FADP applies, the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner.

(vii) with respect to Customer Data to which the Canada Privacy Law applies, the competent supervisory authority is the Office of the Privacy Commissioner of Canada.

Annex 2: Description of Transfer

Personal data that will be processed according to the scope of the Service Agreement and related Statement(s) of Work the purposes for which these data will be processed is defined as follows:

Subject Matter: Device Management and Remote Administration on behalf of the Customer.

Purpose of processing: Vendor may process Personal data on behalf of the Customer in order facilitate Neat Pulse (Services) on behalf of the Customer and includes:

- 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.

Nature of data processing: Personal data may be processed according to the Service Agreement and affiliated Statement(s) of Work to support the managed services, and the processing activity may involve collection, storage, duplication, electronic viewing, media streaming, deletion, and destruction of personal data.

Categories of Data Subjects: The categories of data subjects may include the following:

- Workforce (employees, contractors, agents etc.) of End Customer

Categories of personal data transferred:

CRM Data:

Personal data that may be collected, processed and transferred related to customer relationship activities, such as service provisioning, sales, marketing, customer success, professional services, support.

- Full Name
- Email Address
- Region or Country

Service Provisioning Data:

Personal data that may be collected for provisioning users within Neat Pulse include:

- User ID
- Full Name
- Email Address
- User Role (Owner, Admin)
- Authentication data (only system identifier)

Device Data:

Personal data may be provided by the users while configuring the devices. Device names can reflect the job title or name of key managerial personnel and IP details of devices provisioned in remote working environment may be Personal data.

- Device Name
- Network Identifiers such as IP Address, MAC Address, Bluetooth Address, etc.
- Device Log Files – User may choose to submit unstructured log files generated by Neat devices to Neat Support for troubleshooting purposes. This log file is encrypted before transmission.

Audit Log Data:

- The Audit Logs generated by the Services which capture the user activities, IP address for support and tracking purposes.

Usage Analytics Data:

- Information collected by the Analytics provider in the categories of device data, online activity data, communications data, location information.
- Pulse specific data that may be matched against Analytics data include
    - Tenant ID
    - Tenant Name
    - Pulse generated User ID
    - Pulse license level

Transient Data accessible via Neat Pulse:

There are two categories of data that are **not stored** in Neat Pulse data store but can be accessed by the remote administrator when they remotely access the device. They are:

1. Company Contact Data (Specific to Neat Pad device only)
   a. Full Name
   b. Email address.

2. Communications Data

   The application provider data (Microsoft Teams, Zoom, Google Meet etc.) can be accessed while the meeting is in progress, and they are **not persisted** in the device or Neat Pulse data store.

   - The Meeting Participant Data which includes Full Name, Company Name and Email address.
   - The video media stream of the meeting apart from the content shared in the meeting.

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.

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.

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

Continuous.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

All data will be retained up to ninety days after the end of the contractual relationship, in compliance with data protection and data security policies and in accordance with the instructions of the Customer and the applicable data retention laws.

Annex 3: Security Measures

Annex 3 describes the adopted security measures cemented in an Information Security Management System (ISMS) for the purpose of protecting Personal Data and information, primarily with a view to meeting pre-defined requirements of applicable data protection and privacy law across Controller markets. These requirements have largely been derived from legislation across Controller markets mandating fundamental security measures for the protection of Personal Data and are intended to provide a harmonised and single standard.

These requirements are applied for the protection of Personal Data on behalf of the Customer.

Security Officer

1. A person responsible for the overall compliance with these minimum-security requirements shall be designated as the Security Officer. This person shall be suitably trained and experienced in managing information security and provided with appropriate resources to effectively ensure compliance.
2. The contact details of the Security Officer shall be promptly provided to the Customer.

Security Plan and Document

3. The measures adopted to comply with these minimum-security requirements shall be the subject of a security plan and set out in a security document, which shall be kept up to date, and revised whenever relevant changes are made to the Information System or to how it is organised. The security document shall record significant changes to the security measures or the processing activities.
4. The security plan shall address security measures relating to the modification and maintenance of the system used to Process Personal Data, including the development and maintenance of applications, appropriate vendor support, an inventory of hardware and software, and physical security, including security of the buildings or premises where data Processing occurs, security of data equipment and telecommunication infrastructure and environmental controls.
5. Data security mechanisms for securing the integrity and confidentiality of the data, classification of the data.
6. Security of computers and telecommunication systems including procedures for managing back-up copies, procedures dealing with computer viruses, procedures for managing signal/codes, security for software implementation, security related to databases, security for connecting systems to the Internet, inspection of circumvention of data system, mechanisms for keeping account of attempts to break system security or gain unauthorized access.
7. The security plan shall include:
    a. a Disaster Recovery Plan which shall set out: measures to minimize interruptions to the normal functioning of the system; limit the extent of any damage and disasters; enable a smooth transition of Personal Data from one computer system to another; if necessary, provide for alternative means of operating a computer system; educate, exercise and familiarize personnel with emergency procedures; provide for fast and smooth system recovery, and minimize the economic effects of any disaster event.

    b. a Contingency Plan which must address the following possible dangers to the system and appropriate criteria to determine when the Plan must be triggered: the critical functions and systems, the strategy for protecting the system and priorities in the event the Plan is activated; an inventory of relevant staff members to be called upon during an emergency, as well as telephone numbers of other relevant parties; a set of procedures for calculating the damage incurred; realistic time management plans to enable the recovery of the system; clearly allocated staff duties; possible use of alarms and special devices (e.g., air filters, noise filters); in the event of a fire, special equipment must be available (e.g., fire extinguisher, water pumps, etc.); devices or methods for determining temperature, humidity and other environmental factors (e.g., air conditioning, thermometers, etc.); special security software to detect breaches of security; special generators for dealing with power cuts; retention of copies of software or materials in other protected buildings to avoid inadvertent loss.

8. The security document shall be available to staff who have access to Personal Data and the Information Systems, and must cover the following aspects as a minimum:

    a. The scope, with a detailed specification of protected resources;

    b. The measures, standards, procedures, code of conduct rules and norms to guarantee security, including for the control, inspection and supervision of the Information Systems;

    c. The functions and obligations of staff;

    d. The structure of files containing Personal Data and a description of the Information Systems on which they are Processed;

    e. The purposes for which the Information Systems may be used;

    f. The procedures for reporting, managing and responding to incidents;

    g. The procedures for making back-up copies and recovering data including the person who undertook the process, the data restored and, as appropriate, which data had to be input manually in the recovery process.

9. The security document and any related records and documentation shall be retained for a minimum period of 5 years from the end of the Processing.

Functions and Obligations of Staff

10. Only those employees who have demonstrated honesty, integrity and discretion will be Authorised Users or have access to premises where Information Systems or media containing Personal Data are located. Staff will be bound by a duty of confidentiality in respect of any access to Personal Data.

11. The necessary measures shall be adopted to train and make staff familiar with these minimum-security requirements, any relevant policies and applicable laws concerning the performance of their functions and duties in respect of the Processing of Personal Data and the consequences of any breach of these requirements.

12. The functions and obligations of staff having access to Personal Data and the Information Systems shall be clearly defined and documented.

13. Authorised Users shall be instructed to the effect that electronic equipment must not be left unattended and made accessible during Processing sessions.

14. Physical access to areas where any Personal Data are stored shall be restricted to Authorised Users.

15. The disciplinary measures for a breach of the security plan shall be clearly defined and documented and communicated to staff.

Authorisation

16. Only those employees who have a legitimate operational need to access the Information Systems or carry out any Processing of Personal Data shall be authorised to do so (“Authorised Users”).

17. An authorisation system shall be used where different authorisation profiles are used for different purposes.

Identification

18. Every Authorised User must be issued with a personal and unique identification code for that purpose (“User ID”).

19. A User ID may not be assigned to another person, even at a subsequent time.

20. An up-to-date record shall be kept of Authorised Users, and the authorised access available to each, and identification and authentication procedures shall be established for all access to Information Systems or for carrying out any Processing of Personal Data.

Authentication

21. Password is handled using Azure B2C and is not stored in Neat Pulse datastore. Neat Pulse holds only hash and system identifiers used in the authentication process.

22. Authorised Users shall be allowed to Process Personal Data if they are provided with authentication credentials such as to successfully complete an authentication procedure relating either to a specific Processing operation or to a set of Processing operations.

23. Authentication must be based on a secret password associated with User ID, and which password shall only be known to the Authorised User; alternatively, authentication shall consist in an authentication device that shall be used and held exclusively by the person in charge of the Processing and may be associated with either an ID code or a password, or else in a biometric feature that relates to the person in charge of the Processing and may be associated with either an ID code or a password.

24. One or more authentication credentials shall be assigned to, or associated with, an Authorised User.

25. There must be a procedure that guarantees password confidentiality and integrity. Passwords must be stored in a way that makes them unintelligible while they remain valid. There must be a procedure for assigning, distributing and storing passwords.

26. Passwords shall consist of at least eight characters, or, if this is not technically permitted by the relevant Information Systems, a password shall consist of the maximum permitted number of characters. Passwords shall not contain any item that can be easily related to the Authorised User in charge of the Processing and must be changed at regular intervals, which intervals must be set out in the security document. Passwords shall be modified by the Authorised User to a secret value known only to the Authorised User when it is first used.

27. The instructions provided to Authorised Users shall lay down the obligation, as a condition of accessing the Information Systems, to take such precautions as may be necessary to ensure that the confidential component(s) in the credentials are kept secret and that the devices used and held exclusively by Authorised Users are kept with due care.

28. Authentication credentials shall be de-activated if they have not been used for at least six months, except for those that have been authorised exclusively for technical management and support purposes.

29. Authentication credentials shall be also de-activated if the Authorised User is disqualified or de-authorised from accessing the Information Systems or Processing Personal Data.

30. Where data and electronic equipment may only be accessed by using the confidential component(s) of the authentication credential, appropriate instructions shall be given in advance, in writing, to clearly specify the mechanisms by which the exporter can ensure that data or electronic equipment are available in case the person in charge of the Processing is either absent or unavailable for a long time and it is indispensable to carry out certain activities without further delay exclusively for purposes related to system operationality and security. In this case, copies of the credentials shall be kept in such a way as to ensure their confidentiality by specifying, in writing, the entities in charge of keeping such credentials. Such entities shall have to inform the person in charge of the Processing, without delay, as to the activities carried out.

Access Controls

31. Only Authorised Users shall have access to Personal Data, including when stored on any electronic or portable media or when transmitted. Authorised Users shall have authorised access only to those data and resources necessary for them to perform their duties.

32. A system for granting Authorised Users access to designated data and resources shall be used.

33. Authorisation profiles for each individual Authorised User or for homogeneous sets of Authorised Users shall be established and configured prior to the start of any Processing in such a way as to only enable access to data and resources that are necessary for Authorised Users to perform their duties.

34. It shall be regularly verified, at least at yearly intervals, that the prerequisites for retaining the relevant authorisation profiles still apply. This may also include the list of Authorised Persons drawn up by homogeneous categories of task and corresponding authorisation profile.

35. Measures shall be put in place to prevent a user gaining unauthorised access to, or use of, the Information Systems. In particular, firewalls and/or intrusion detection systems reflecting the state of the art and industry best practice must be installed to protect the Information Systems from unauthorized access. Measures shall be put in place to identify when the Information Systems have been accessed or Personal Data has been Processed without authorization, or where there have been unsuccessful attempts at the same.

36. Operating system or database access controls must be correctly configured to ensure authorised access.

37. Only those staff authorised in the security document shall be authorised to grant, alter or cancel authorised access by users to the Information Systems.

Management of Media

38. Information Systems and physical media storing Personal Data must be housed in a secure physical environment. Measures must be taken to prevent unauthorized physical access to premises housing Information Systems.

39. Organisational and technical instructions shall be issued with regard to keeping and using the removable media on which the data are stored in order to prevent unauthorised access and Processing.

40. Media containing Personal Data must permit the kind of information they contain to be identified, Inventoried (including the time of data entry; the Authorised User who entered the data and the person from whom the data was received; and the Personal Data entered) and stored at a physical location with physical access restricted to staff that are authorised in the security document to have such access.

41. When media are to be disposed of or reused, the necessary measures shall be taken to prevent any subsequent retrieval of the Personal Data and other information stored on them, or to otherwise make the information intelligible or be re-constructed by any technical means before they are withdrawn from the inventory. All reusable media used for the storage of Personal Data must be overwritten three times with randomised data prior to disposal or re-use.

42. The removal of media containing Personal Data from the designated premises must be specifically authorised by the Customer.

43. Media containing Personal Data must be erased or rendered unreadable if it is no longer used or prior to disposal.

Distribution of Media and Transmission

44. Media containing Personal Data must only be available to Authorised Users.

45. Printing/copying Processes must be physically controlled by Authorised Users, to ensure that no prints or copies containing Personal Data remain left in the printers or copying machines.

46. Media containing Personal Data or printed copies of Personal Data must contain the classification mark “Confidential”.

47. Encryption (128-bit or stronger) or another equivalent form of protection must be used to protect Personal Data that is electronically transmitted over a public network or stored on a portable device, or where there is a requirement to store or Process Personal Data in a physically insecure environment.

48. All communications with Neat Pulse are encrypted via industry standard HTTPS/TLS (TLS 1.2 or higher) over public networks. This ensures that all traffic between devices and Neat Pulse is secure during transit. TLS certificates are managed with best practices such as short expiration dates and weekly renewal. All data stored on the Pulse cloud service is encrypted at rest using AES 256-bit encryption. This includes all databases, image files, log files, and more.

49. Users may choose to submit unstructured device log files generated by the Neat devices to Neat Pulse for troubleshooting purposes. This log file is encrypted before transmission.

50. Paper documents containing Personal Data must be transferred in a sealed container / envelope that indicates clearly that the document must be delivered by hand to an Authorised User.

51. When media containing Personal Data are to leave the designated premises as a result of maintenance operations, the necessary measures shall be taken to prevent any unauthorised retrieval of the Personal Data and other information stored on them.

52. A system for recording incoming and outgoing media must be set up which permits direct or indirect identification of the kind of media, the date and time, the sender/recipient, the number of media, the kind of information contained, how they are sent and the person responsible for receiving /sending them, who must be duly authorised.

53. Where Personal Data is transmitted or transferred over an electronic communications network, measures shall be put in place to control the flow of data and record the timing of the transmission or transfer, the Personal Data transmitted or transferred, the destination of any Personal Data transmitted or transferred, and details of the Authorised User conducting the transmission or transfer.

Preservation, Back-up copies and Recovery

54. Tools must be in place to prevent the unintended deterioration or destruction of Personal Data.

55. Procedures must be defined and laid down for making back-up copies and for recovering data. These procedures must guarantee that Personal Data files can be reconstructed in the state they were in at the time they were lost or destroyed.

56. Back-up copies must be made at least once a week unless no data has been updated during that period.

57. The database used maintains three local redundant synchronous copies of the database files to ensure data durability. Where appropriate, high availability (HA) architectural patterns are used to ensure automatic failover and scaling.

Anti-Virus / Intrusion Detection

58. Anti-virus software or intrusion detection systems must be installed on the Information Systems to protect against attacks or other unauthorised acts in respect of Information Systems. Antivirus software and intrusion detection systems must be updated regularly in accordance with the state of the art and industry best practice for the Information Systems concerned (and at least every six months).

Software Updates

59. The software, firmware and hardware used in the Information Systems shall be reviewed regularly in order to detect vulnerabilities and flaws in the Information Systems and resolve such vulnerabilities and flaws. This review shall be carried out at least annually.

60. Pulse makes heavy use of Microsoft Azure, ensuring underlying systems are managed and up to date. This means application and operating system patches are managed automatically by Azure. When new components are created, they are designed to make use of such managed services, minimizing the operational complexity and therefore increasing the overall security of the system.

61. The Pulse architecture is designed to minimize data sharing. Each organization or tenant's data is stored in its own independent database. Architectural decisions follow a collaborate design process, security and privacy review, and require sign-off by the senior level of engineering before implementation.

62. Software is developed using the modern collaboration features of GitHub. Source code is stored on GitHub, guaranteeing change history, availability, and resilience of the assets. Changes are peer reviewed before being merged into a release, and changes are accompanied by unit and integration tests suitable for the feature or fix. Tests are run on every change (continuous integration) and software releases are only produced if all tests pass. Every successfully tested build automatically results in a new release (continuous delivery), which can be deployed to production quickly and easily.

Access Record

63. A history of Authorised Users' access to or disclosure of Personal Data shall be recorded on a secure audit trail.

64. Neat Pulse captures user activities at granular level including that of the remote personnel who access the devices. This event log is available for view by provisioned users in Neat Pulse and it helps in non-repudiation of events. Vendor also ensures separation of roles that system's users who get direct access to database do not act as remote personnel trouble shooting the devices.

Physical Access Record

65. Only those staff duly authorised in the security document may have physical access to the premises where Information Systems and media storing Personal Data are stored. A record of staff who access such premises shall be maintained, including name, date, and time of access.

Record of Incidents

66. There shall be a procedure for reporting, responding to and managing security incidents such as data security breaches or attempts at unauthorised access. This shall include as a minimum:

    a. A procedure for reporting such incidents/ breaches to appropriate management within the Vendor;

    b. A clearly designated team for managing and co-ordinating the response to an incident led by the Security Officer;

    c. A documented and tested process for managing the response to an incident including the requirement to keep appropriate issues and action logs to include the time at which the incident occurred, the person reporting the incident, to whom it was reported and the effects thereof;

    d. The requirement on the Vendor to notify the Customer immediately if it appears that Personal Data was involved in the incident or breach or may be impacted or affected in some way; and

    e. The Vendor security/ incident management team must, where appropriate, work together with the Customer's security representatives until the incident or breach has been satisfactorily resolved.

Annex 4: List of Approved Subprocessors

The following subprocessors have been vetted and may be involved in aspects of processing PII according to the instructions of the organisation.

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

ANNEX 5 – CCPA - PERSONAL INFORMATION PROCESSING PURPOSES AND DETAILS

Contracted Business Purposes: The purposes mentioned in Annex 2 of this DPA for which the Service Provider receives or accesses personal information.
Personal Information Categories: This Addendum involves the following types of Personal Information, as defined and classified in CCPA Cal. Civ. Code § 1798.140(o).

Category	**Examples**	**Processed under this Addendum**
A. Identifiers.	A real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, Social Security number, driver's license number, passport number, or other similar identifiers.	YES
B. Personal information categories listed in the California Reseller Records statute (Cal. Civ. Code § 1798.80(e)).	A name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information. Some personal information included in this category may overlap with other categories.	YES
C. Protected classification characteristics under California or federal law.	Age (40 years or older), race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, veteran or military status, genetic information (including familial genetic information).	NO
D. Commercial information.	Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.	NO
E. Biometric information.	Genetic, physiological, behavioral, and biological characteristics, or activity patterns used to extract a template or other identifier or identifying information, such as fingerprints, faceprints, and voiceprints, iris or retina scans, keystroke, gait, or other physical patterns, and sleep, health, or exercise data.	NO
F. Internet or other similar network activity.	Browsing history, search history, information on a consumer's interaction with a website, application, or advertisement.	NO
G. Geolocation data.	Physical location or movements.	YES
H. Sensory data.	Audio, electronic, visual, thermal, olfactory, or similar information.	NO
I. Professional or employment-related information.	Current or past job history or performance evaluations.	NO
J. Non-public education information (per the Family Educational Rights and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R. Part 99)).	Education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules, student identification codes, student financial information, or student disciplinary records.	NO

K. Inferences drawn from other personal information.	Profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.	NO