Data Processing Addendum

This Data Processing Addendum (this "**DPA**") supplements the Master Subscription Agreement (the "**Agreement**") by and between Trove Information Technologies, Inc. dba Pave ("**Pave**") and the customer named in the Agreement ("**Customer**"), and is incorporated into and forms part of the Agreement. Any term not defined in this DPA shall have the meaning set forth in the Agreement. Pave and Customer hereby agree that the following terms govern Pave's processing of, and Customer's provision to Pave of, any Personal Data (as defined below) pursuant to the Agreement.

1. Definitions

"**Affiliate**" means (a) an entity of which a party directly or indirectly owns fifty percent (50%) or more of the stock or other equity interest, (b) an entity that owns at least fifty percent (50%) or more of the stock or other equity interest of a party or (c) an entity which is under common control with a party by having at least fifty percent (50%) or more of the stock or other equity interest of such entity and a party owned by the same person, but such entity shall only be deemed to be an Affiliate so long as such ownership exists.

"**Aggregated and De-Identified Data**" shall have the meaning set forth in the Agreement.

"**Data Protection Laws**" means any applicable laws and regulations in any relevant jurisdiction relating to the processing of Personal Data including: (a) the California Consumer Privacy Act, as amended by the California Privacy Rights Act, along with its associated regulations (the "**CCPA**"), (b) the General Data Protection Regulation (Regulation (EU) 2016/679) (the "**EU GDPR**" or "**GDPR**"), (c) the Swiss Federal Act on Data Protection, (d) the EU GDPR as it forms part of the law of England and Wales by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the "**UK GDPR**"), (e) the UK Data Protection Act 2018, (f) the Privacy and Electronic Communications (EC Directive) Regulations 2003 and (g) similar comprehensive privacy laws in effect in U.S. states other than California (together with the CCPA, "**U.S. State Privacy Laws**"); in each case, as updated, amended or replaced from time to time and including any implementing regulations. For the avoidance of doubt, if Pave's processing activities involving Personal Data are not within the scope of a given Data Protection Law, such law is not applicable for purposes of this DPA.

The terms "**Data Subject**", "**Personal Data Breach**", "**processing**", "**processor**", "**controller**" and "**supervisory authority**" shall have the meanings set forth in the GDPR, unless another Data Protection Law is more directly applicable to the processing than the GDPR, in which case the definitions of these terms or analogous terms in such other law will apply.

"**EU SCCs**" means the standard contractual clauses approved by the European Commission in Commission Decision 2021/914 dated 4 June 2021 for transfers of Personal Data to countries not otherwise recognized as offering an adequate level of protection for Personal Data by the European Commission (as amended and updated from time to time).

"**Personal Data**" includes "personal data," "personal information," "personally identifiable information," and similar terms, as such terms are defined pursuant to Data Protection Laws, that Pave processes pursuant to the Agreement. Personal Data does not include Aggregated and De-Identified Data.

"**Products**" shall have the meaning set forth in the Agreement.

"**Standard Contractual Clauses**" means either or both of the EU SCCs or UK SCCs, as the context requires.

"**UK SCCs**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses.

2. **Roles of the Parties; Customer's Obligations**

2.1 Customer may act either as a data controller (for purposes of the CCPA, a "business," as defined in the CCPA) or data processor (for purposes of the CCPA, a "service provider," as defined in the CCPA). Except as expressly set forth in this DPA, Pave is a data processor (for purposes of the CCPA, a "service provider," as defined in the CCPA). The parties' obligations with respect to these roles are stated below.

2.2 Customer represents and warrants that it shall, in its use of the Products, at all times process Personal Data, and provide instructions for the processing of Personal Data, in compliance with Data Protection Laws, including that:

2.2.1 Customer has taken all steps (including obtaining any consents and providing any notices) that are legally required for it to instruct Pave to process the Personal Data as set forth in the Agreement and this DPA;

2.2.2 Customer is solely responsible for the accuracy, quality and legality of (i) the Personal Data provided to Pave by or on behalf of Customer, (ii) the means by which Customer acquired any such Personal Data and (iii) the instructions it provides to Pave regarding the processing of such Personal Data; and

2.2.3 Customer shall not provide or make available to Pave any Personal Data in violation of the Agreement or Data Protection Laws.

3. **Pave's Processor Obligations**

3.1 Pave shall process Personal Data only (a) on Customer's behalf, (b) for the purposes set forth in the Agreement and/or Schedule A, (c) in accordance with the Agreement, this DPA or any other documented instructions provided by Customer and (d) in compliance with Data Protection Laws. Customer hereby instructs and permits Pave to process Personal Data in accordance with the foregoing and as part of any processing initiated by Customer in its use of the Products, including by aggregating and de-identifying Personal Data in order to facilitate such purposes.

3.2 Pave shall promptly notify Customer if an instruction of Customer, in Pave's opinion, infringes Data Protection Laws.

3.3 As required under U.S. State Privacy Laws, Pave will:

3.3.1 not retain, use or disclose the Personal Data outside of the direct business relationship between Customer and Pave or for any purpose (including any commercial purpose) not set forth in this DPA;

3.3.2 not "sell" or "share" any Personal Data or use Personal Data for purposes of "targeted advertising", as such terms are defined in U.S. State Privacy Laws;

3.3.3 not attempt to re-identify any pseudonymized, anonymized, aggregate or de-identified Personal Data without Customer's express written permission;

3.3.4 comply with any applicable restrictions on combining Personal Data with personal data that Pave receives from, or on behalf of, another person or persons, or that Pave collects from any interaction between it and any individual;

3.3.5 provide at least the same level of protection for Personal Data as is required under U.S. State Privacy Laws;

3.3.6 not otherwise engage in any processing of Personal Data that is prohibited or not permitted by "processors" or "service providers"; and

3.3.7 promptly notify Customer if Pave determines that it (i) can no longer meet its obligations under this DPA or Data Protection Laws or (ii) has breached this DPA, and shall cooperate to remediate such breach.

3.3.8 Where permitted under the CCPA, Customer may, upon notice, take reasonable steps to (a) remediate unauthorized use of Personal Data subject to the CCPA and (b) ensure Pave processes Personal Data subject to the CCPA in a manner consistent with Customer's obligations under the CCPA.

3.4 Notwithstanding anything in this Section 3, if Pave is required to process Personal Data in a manner inconsistent with this DPA by the laws or supervisory authority to which Pave is subject, it may do so; in such a case, Pave shall inform Customer of that legal requirement before such processing, unless relevant law prohibits doing so on important grounds of public interest.

3.5 The subject matter, nature, purpose and duration of processing, as well as the types of Personal Data processed and categories of Data Subjects, are described in Schedule A.

3.6 On termination or expiration of the Agreement, Pave shall, at Customer's choice, return or delete the Personal Data. If return or destruction of Personal Data is unfeasible or prohibited by law, rule or regulation, Pave shall take measures to permanently render unreadable or inaccessible such Personal Data (except to the extent necessary for its continued hosting or processing as required by law, rule or regulation) and this DPA shall continue to apply to such Personal Data as long as it remains in Pave's possession, custody or control. If Customer and Pave have entered into Standard Contractual Clauses as described in Section 7 (*Transfers of Personal Data*), the parties agree that the certification of deletion of Personal Data that is described in Clause 8.1(d) and Clause 8.5 of the EU SCCs shall be provided by Pave to Customer only upon Customer's request.

4. Confidentiality

Pave shall process Personal Data subject to the confidentiality provisions of the Agreement. Pave shall ensure that any person it authorizes to process Personal Data has agreed to protect Personal Data in accordance with Pave's confidentiality obligations in the Agreement.

5. Sub-Processors

5.1 Customer acknowledges and agrees that Pave may engage its Affiliates and other subcontractors to process Personal Data in accordance with the provisions of this DPA and Data Protection Laws ("**Sub-Processors**"). By agreeing to this DPA, Customer provides general written authorization to Pave to engage (a) the Sub-Processors listed at https://www.pave.com/subprocessors (the "**Sub-Processor List**") and (b) Sub-Processors subsequently added to the Sub-Processor List to which Customer does not object in accordance with this Section 5.

5.2 Pave may add Sub-Processors to the Sub-Processor List from time to time in accordance with the terms of this DPA. Pave may provide a mechanism to subscribe to notifications of new Sub-Processors and Customer agrees to subscribe to such notifications where available. At least ten (10) days before enabling a new Sub-Processor to process Personal Data, Pave will add such new Sub-Processor to the Sub-Processor List and notify Customer. Within ten (10) days of receiving such notice, Customer may notify Pave in writing of any objection to the engagement of the new Sub-Processor based on the reasonable belief that the new Sub-Processor will not be able to provide an appropriate level of protection to Personal Data. Customer acknowledges that certain Sub-Processors are essential to providing the Products and that objecting to the use of a Sub-Processor may prevent Pave from offering the Products to Customer.

5.3 If Customer reasonably objects to Pave engaging a Sub-Processor in accordance with Section 5.2 and Pave cannot provide a commercially reasonable alternative within a reasonable period of time, Customer may discontinue the use of the affected Product(s) (but not any unaffected Product) by providing prior

written notice to Pave. Customer may receive a refund of pre-paid Fees for subscriptions to the affected Product(s) (but not any unaffected Product) that would have been provided after the date of discontinuation.

5.4 If Customer does not object to the engagement of a new Sub-Processor in accordance with Section 5.2, that new Sub-Processor will be authorized to process the Personal Data.

5.5 Pave will enter into a written agreement with the new Sub-Processor imposing data protection obligations substantially similar to those imposed on Pave under this DPA with respect to the protection of Personal Data. In case a Sub-Processor fails to fulfill its data protection obligations under such written agreement with Pave, Pave will remain liable to Customer for such failure.

5.6 If Customer and Pave have entered into Standard Contractual Clauses as described in Section 7 (*Transfers of Personal Data*), (a) the above authorizations will constitute Customer's prior written consent to the subcontracting by Pave of the processing of Personal Data if such consent is required under the Standard Contractual Clauses and (b) the parties agree that the copies of the agreements with Sub-Processors that must be provided by Pave to Customer pursuant to Clause 9(c) of the EU SCCs may have commercial information, or information unrelated to the Standard Contractual Clauses or their equivalent, removed by Pave beforehand, and that such copies will be provided by Pave only upon written request by Customer.

6. Security of Personal Data

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, Pave shall maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk of processing Personal Data. Schedule C sets forth additional information about Pave's technical and organizational security measures.

7. Transfers of Personal Data

7.1 The parties agree that Pave may transfer Personal Data processed under this DPA outside the EEA, the UK or Switzerland as necessary to provide the Products. Customer acknowledges that Pave's primary processing operations take place in the United States, and that the transfer of Personal Data to the United States is necessary for the provision of the Products to Customer. If Pave transfers Personal Data protected under this DPA to a jurisdiction for which the European Commission has not issued an adequacy decision, Pave will ensure that appropriate safeguards have been implemented for the transfer of Personal Data in accordance with Data Protection Laws.

7.2 **Transfers of EEA Personal Data.** To the extent legally required, the EU SCCs are deemed incorporated into this DPA by reference and take precedence over the rest of this DPA to the extent of any conflict. The EU SCCs are completed as follows:

7.2.1 *Module Two (Controller to Processor)* of the EU SCCs apply when Customer is a controller and Pave is processing Personal Data for Customer as a processor.

7.2.2 *Module Three (Processor to Sub-Processor)* of the EU SCCs apply when Customer is a processor and Pave is Customer's sub-processor.

7.2.3 For each module, where applicable, the following applies:

7.2.4 The optional docking clause in Clause 7 does not apply;

7.2.5 In Clause 9, Option 2 (*general written authorization*) applies, and the minimum time period for prior notice of sub-processor changes shall be as set forth in Section 5.2 of this DPA;

7.2.6 In Clause 11, the optional language does not apply;

7.2.7 In Clause 17 (*Option 1*), the EU SCCs will be governed by Irish law;

7.2.8 In Clause 18(b), disputes will be resolved before the courts of Ireland;

7.2.9 Schedule B to this DPA contains the information required in Annex I of the EU SCCs;

7.2.10 Schedule C to this DPA contains the information required in Annex II of the EU SCCs; and

7.2.11 By entering into this DPA, the parties are deemed to have signed the EU SCCs incorporated herein, including their Annexes.

7.3 **Transfers of UK Personal Data.** To the extent legally required, with respect to Personal Data transferred from the United Kingdom for which United Kingdom law (and not the law in any European Economic Area jurisdiction) governs the international nature of the transfer, the UK SCCs are incorporated into this DPA by reference and take precedence over the rest of this DPA to the extent of any conflict. The Tables of the UK SCCs are completed as follows:

7.3.1 Table 1: The parties' details are the parties and their Affiliates to the extent any of them are involved in such a transfer, including those set forth in Schedule B of this DPA. The Key Contacts shall be the contacts set forth in Schedule B of this DPA.

7.3.2 Table 2: The Approved EU SCCs referenced in Table 2 shall be the EU SCCs as set forth in Section 7.2 of this DPA.

7.3.3 Table 3: Annexes I and II shall be set forth in Schedules B and C to this DPA, respectively. Annex III is inapplicable.

7.3.4 Table 4: Pave may end this Section 7.3 (thereby terminating the UK SCCs as between the parties) as set out in Section 19 of the UK SCCs.

7.4 **Transfers from Switzerland.** The parties agree that transfers from Switzerland are made pursuant to the EU SCCs with the following modifications:

7.4.1 The terms "General Data Protection Regulation" or "Regulation (EU) 2016/679" as utilized in the EU SCCs shall be interpreted to include the Federal Act on Data Protection (the "**FADP**") with respect to data transfers subject to the FADP.

7.4.2 Clause 13 of the EU SCCs is modified to provide that the Federal Data Protection and Information Commissioner ("**FDPIC**") of Switzerland shall have authority over data transfers to the extent they are governed by the FADP and the appropriate EU supervisory authority shall have authority over data transfers to the extent they are governed by the GDPR.

7.4.3 The term "EU Member State" as utilized in the EU SCCs shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from exercising their rights in their place of habitual residence in accordance with Clause 18(c) of the EU SCCs.

7.5 **Supplementary Measures.** In respect of any transfer of EEA or UK Personal Data, the following supplementary measures shall apply:

7.5.1 As of the date of this DPA, Pave has not received any formal legal requests from any government intelligence or security service/agencies in the country to which the Personal Data is being exported, for access to (or for copies of) Personal Data ("**Government Agency Requests**").

7.5.2 If, after the date of this DPA, Pave receives any Government Agency Requests, Pave shall attempt to redirect the law enforcement or government agency to request that data directly from Customer. As part of this effort, Pave may provide Customer's basic contact information to the government agency. If compelled to disclose Personal Data to a law enforcement or government agency, Pave shall give Customer reasonable notice of the demand and cooperate to allow Customer to seek a protective order or other appropriate remedy unless Pave is legally prohibited from doing so. Pave shall only disclose Personal Data to any law enforcement or government agency if legally obligated to do so after Pave has made commercially reasonable efforts to challenge the relevant disclosure

request, and shall only disclose the minimum amount of Personal Data necessary to comply with such request.

7.5.3 If either (i) any of the means of legitimizing transfers of Personal Data outside of the EEA or UK set forth in this DPA cease to be valid or (ii) any supervisory authority requires transfers of Personal Data pursuant to those means to be suspended, then Pave may by notice to Customer, with effect from the date set out in such notice, amend or put in place alternative arrangements in respect of such transfers, as required by Data Protection Laws.

8. **Rights of Data Subjects**

8.1 Pave shall, to the extent permitted by law, notify Customer upon receipt of a request by a Data Subject to exercise any of the Data Subject's rights under Data Protection Laws (individually and collectively "**Data Subject Request(s)**"). If Pave receives a Data Subject Request in relation to Personal Data, Pave will advise the Data Subject to submit their request to Customer and Customer will be responsible for responding to such request, including, where necessary, by using the functionality of the Products. Customer is solely responsible for ensuring that Data Subject Requests for erasure, restriction or cessation of processing, or withdrawal of consent to processing of any Personal Data are communicated to Pave.

8.2 Pave shall, at the request of Customer and taking into account the nature of the processing applicable to any Data Subject Request, provide reasonable assistance to enable Customer to comply with Customer's obligation to respond to such Data Subject Request and/or in demonstrating such compliance, where possible, only to the extent that (a) Customer is itself unable to respond without Pave's assistance, (b) Pave is able to do so in accordance with all applicable laws, rules and regulations, and (c) Customer shall be responsible for all expenses in connection with any such cooperation or assistance that requires Pave to expend unreasonable time or effort or is otherwise unreasonably burdensome.

9. **Actions and Access Requests; Audits**

9.1 Pave shall, taking into account the nature of the processing and the information available to Pave, provide Customer with reasonable cooperation and assistance where necessary for Customer to comply with its obligations under Data Protection Laws, to conduct a data protection impact assessment, risk assessment, and/or to demonstrate such compliance; provided, however, that (a) Customer does not otherwise have access to the relevant information and (b) Customer shall be responsible for all expenses in connection with any such cooperation or assistance that requires Pave to expend unreasonable time or effort or is otherwise unreasonably burdensome.

9.2 Pave shall, taking into account the nature of the processing and the information available to Pave and at Customer's cost, provide Customer with reasonable cooperation and assistance with respect to prior consultation with any supervisory authority.

9.3 Upon Customer's written request, but no more than once per calendar year and subject to reasonable confidentiality controls, Pave shall either (at Pave's sole option) (a) make available for Customer's review copies of certifications or reports demonstrating Pave's compliance with this DPA or (b) allow Customer's independent third party representative to conduct an audit of Pave's data security practices, only to the extent that (i) Customer provides reasonable prior written notice, (ii) such audit is performed during business hours and is not unreasonably disruptive to Pave's business, (iii) the scope of such audit is reasonable, including, but not limited to, being restricted to data, systems and sites (x) relevant to Customer and (y) which, in Pave's sole discretion, would not compromise Pave's security. Audits are at Customer's expense, including, but not limited to costs, fees and hourly rates. If Customer and Pave have entered into Standard Contractual Clauses as described in Section 7 (*Transfers of Personal Data*), the

parties agree that the audits described in Clause 8.9 of the EU SCCs shall be carried out in accordance with this section.

9.4 In the event of a Personal Data Breach that affects Personal Data, Pave shall, taking into account the nature of the processing and the information available to Pave:

9.4.1 without undue delay, and in any event within seventy-two (72) hours of becoming aware of such Personal Data Breach, inform Customer of: (a) the nature of the Personal Data Breach, including, where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned; (b) the likely consequences of the Personal Data Breach; and (c) measures taken or proposed to be taken by Pave to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects; and

9.4.2 provide Customer, at its request, with reasonable cooperation and assistance as necessary for Customer to comply with its obligations under Data Protection Laws with respect to notifying the relevant supervisory authority and Data Subjects affected by the Personal Data Breach; provided, however, that Customer will bear the cost of any such assistance that it requests unless the Personal Data Breach is caused by Pave's intentional or negligent violation of this DPA or Data Protection Laws.

9.5 The obligations described in this Section 9.4 shall not apply in the event that a Personal Data Breach is directly and proximately caused by any act or omission on the part of Customer. Pave's obligation to report or respond to a Personal Data Breach will not be construed as an acknowledgement by Pave of any fault or liability with respect to the Personal Data Breach.

10. **Conflict**

In the event of any conflict or inconsistency among the following documents, the order of precedence will be: (a) the applicable terms in the Standard Contractual Clauses, (b) the terms of this DPA and (c) the Agreement. Any claims brought in connection with this DPA will be subject to the terms and conditions, including, but not limited to, the exclusions and limitations set forth in the Agreement.

Schedule A

Details of Processing

Nature and Purpose of Processing: Pave will process Personal Data as necessary to provide the Products under the Agreement, for the purposes specified in the Agreement and this DPA, and in accordance with Customer's instructions as set forth in the Agreement and this DPA. The nature of this processing includes, without limitation, collecting, accessing, storing, organizing, analyzing, modifying, disclosing, returning and/or deleting Personal Data (each as the context requires or permits) and generating Aggregated and De-Identified Data as described in the Agreement.

Duration of Processing: For the duration of the Agreement plus the period from expiry of the Agreement until deletion of Personal Data by Pave in accordance with the Agreement and this DPA.

Categories of Data Subjects: Customer's employees and job candidates.

Categories of Personal Data: The categories of Personal Data depend on the systems that Customer wants to connect to Pave's Products, so these categories may vary depending on the system and the method of integration. Generally speaking, the Personal Data transferred concerns compensation information (e.g., employee salary and benefits data) and names (and/or other unique identifiers, such as employee ID, if applicable) of Customer's employees and candidates.

Sensitive Data or Special Categories of Data: Gender and ethnicity (not applicable for the Market Data Product (previously called the Benchmarking Product), optional for all other Products).

Schedule B

The following includes the information required by Annex I and Annex III of the EU SCCs and Table 3 of the UK SCCs.

1. The Parties

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union*]

Name: *[To be completed by Customer at signing with Customer's full legal entity name]*

Address: *[To be completed by Customer at signing with Customer's registered address]*

Contact person's name, position and contact details: [To be completed by Customer at signing]

Activities relevant to the data transferred under these Clauses: [To be completed by Customer at signing]

Signature and date: By entering into the Agreement, the parties are deemed to have signed this Schedule B.

Role (controller/processor): Controller or Processor, as applicable

Data importer(s):

Name: Trove Information Technologies, Inc. dba Pave

Address: 1 Montgomery St., Suite 700, San Francisco, CA, USA 94104

Contact person's name, position and contact details: Privacy Team, 1 Montgomery St., Suite 700, San Francisco, CA, USA 94104, Attn: Legal

Activities relevant to the data transferred under these Clauses: HR services relating to compensation planning services for Customer's employees and candidates.

Signature and date: By entering into the Agreement, the parties are deemed to have signed this Schedule B.

Role (controller/processor): Processor

2. Description of the Transfer

Data Subjects	Customer's employees and job candidates
Categories of Personal Data	As noted in Schedule A, the categories of Personal Data collected depend on Customer's systems and the methods of integration, but generally include compensation information (e.g., employee salary and benefits information) and names (and/or other unique identifiers, such as employee ID, if applicable) of Customer's employees and candidates
Special Category Personal Data (if applicable)	Gender and ethnicity (not applicable for the Market Data Product (previously called the Benchmarking Product), optional for all other Products)
Nature of the processing	As described in Schedule A

Purposes of processing	To provide a compensation management platform, powered by real-time data, that helps companies benchmark, plan and communicate compensation
Duration of processing and retention (or the criteria to determine such period)	As described in Schedule A
Frequency of the transfer	As necessary to perform all obligations and rights with respect to Personal Data as provided in the Agreement or this DPA
Recipients of Personal Data transferred to the Data Importer	Pave will maintain and provide a list of its Sub-Processors upon request

3. Competent Supervisory Authority

For cross-border transfers governed by the EU SCCs, the competent supervisory authority shall be the Irish Data Protection Commission ("DPC"), consistent with the governing law election in Clause 17 of the EU SCCs. Where Customer's establishment or the location of Data Subjects requires a different lead supervisory authority under Clause 13 of the EU SCCs, the competent authority shall be determined accordingly.

4. List of Sub-Processors

The current list of Sub-Processors is available at https://www.pave.com/subprocessors, which list may be updated from time to time in accordance with this DPA.

Schedule C

Technical and Organizational Security Measures

The following includes the information required by Annex II of the EU SCCs and Table 3 of the UK SCCs.

Technical and Organizational Security Measures	Details
Measures of pseudonymisation and encryption of personal data	Pave encrypts customer data in transit and at rest. Pave uses GCP resources to store and encrypt such data using AES-256. For more information, please see the GCP encryption protocols and documentation at https://cloud.google.com/security/encryption-at-rest.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Pave maintains Business Continuity and Disaster Recovery plans that are tested annually to ensure ongoing confidentiality, integrity, availability and resilience of services.
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	Pave's database is backed up on a daily basis to enable a 24 hour RTO and RPO. Backups are stored on Google Cloud Platform and are retained for a minimum of 6 months. For more information, please see Pave's full data loss prevention policy (available upon request).
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	Pave undergoes annual SOC testing and is currently SOC 2, Type II certified. Pave also undergoes biannual penetration testing by a reputable third-party firm. Pave maintains a bug bounty program.
Measures for user identification and authorization	Pave employees must use two factor authentication to access the corporate or production environment. Customers may enforce authorization requirements via Google OAuth.
Measures for the protection of data during transmission	Pave encrypts customer data in transit. Pave requires TLS 1.2.
Measures for the protection of data during storage	Pave encrypts customer data at rest. Pave uses GCP resources to store and encrypt such data using AES-256. For more information, please see the GCP encryption protocols and documentation at https://cloud.google.com/security/encryption-at-rest.
Measures for ensuring physical security of locations at which personal data are processed	Pave relies on Google for the physical security of its data centers. Google's policies describe its physical security practices.

Technical and Organizational Security Measures	Details
Measures for ensuring events logging	Pave uses DataDog, Sentry and internal tools for logging. Pave has a 365 day retention policy set for Pave's logs.
Measures for ensuring system configuration, including default configuration	Pave's infrastructure configuration is defined in code and maintained in accordance with Pave's Change Management policy, which requires peer reviewers and automated testing.
Measures for internal IT and IT security governance and management	Pave's Head of Security is responsible for overseeing the security program.
Measures for certification/assurance of processes and products	Pave is currently SOC 2, Type II certified.
Measures for ensuring data minimization	Pave only collects and stores data required to perform services and provide products to customers.
Measures for ensuring data quality	Pave uses automated testing and monitoring to ensure data quality.
Measures for ensuring limited data retention	Pave deletes Customer Data upon Customer request in accordance with our Data Deletion Policy. Aggregated and De-Identified Data may be retained in static form for data analysis, research and product purposes.
Measures for ensuring accountability	All employees undergo security training during onboarding and at annual intervals. Violations of company policies may result in disciplinary action.
Measures for allowing data portability and ensuring erasure	Pave provides the option for customers to delete data on request. The underlying data generated by Pave is sourced from a customer's own systems. By the API nature of these systems, these are completely portable to any other vendor.
Technical and organizational measures of sub-processors	Pave enters into data processing agreements with its Sub-Processors with data protection obligations substantially similar to those contained in this DPA.