Last updated: 6/18/2025

DashLoc
DATA PROTECTION ADDENDUM

This Data Protection Addendum ("**Addendum**") between DashLoc ("**Infofavor Solutions Pvt. Ltd.**" Referred as DashLoc, **We or Us**) and the Customer (as defined in the Agreement) forms part of the DashLoc Terms of Service set forth at https://dashloc.com/privacy-policy or such other written or electronic agreement incorporating this Addendum, in each case governing Customer's access to and use of the Services (the "**Agreement**").

Customer enters into this Addendum 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 DashLoc For the purposes of this Addendum only, and except where otherwise indicated, references to "Customer" shall include Customer and such Affiliates.

The Parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Agreement.

1. Definitions

1.1. In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

(a) "**Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with either Customer or DashLoc (as the context allows), where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise;

(b) "**Customer Personal Data**" means any Personal Data provided by or made available by Customer to DashLoc or collected by DashLoc on behalf of Customer which is Processed by DashLoc to perform the Services;

(c) "**Controller to Processor SCCs**" means the standard contractual clauses for cross-border transfers published by the European Commission on June 4, 2021 governing the transfer of European Area Personal Data to Third Countries as adopted by the European Commission, the Swiss Federal Data Protection and Information Commissioner ("**Swiss FDPIC**") relating to data transfers to Third Countries (collectively "**EU SCCs**"); (ii) the international data transfer addendum ("**UK Transfer Addendum**") adopted by the UK Information Commissioner's Office ("**UK ICO"**) for data transfers from the UK to Third Countries; or (iii) any similar such clauses adopted by a data protection regulator relating to Personal Data transfers to Third Countries, including without limitation any successor clauses thereto;

(d) "**Data Protection Laws**" means any local, state, or national law regarding the processing of Personal Data applicable to DashLoc in the jurisdictions in which the Services are provided to Customer, including, without limitation, privacy, security, and data protection law;

(e) "**EU Area**" means the European Union, European Economic Area, United Kingdom, and Switzerland;

(f) "**EU Area Law**" means (i) Directive 95/46/EC and, from May 25, 2018, Regulation (EU) 2016/679 ("**EU GDPR**") together with applicable legislation implementing or supplementing the same or otherwise relating to the processing of Personal Data of natural persons; (ii) the Data Protection Act 1998 of the United Kingdom and the EU GDPR as saved into United Kingdom Law by virtue of section 3 of the

United Kingdom's European Union (Withdrawal) Act 2018 (the "**UK GDPR**"); (iii) the swiss Federal Data Protection Act of 19 June 1992 and its Ordinance ("**Swiss DPA**"); (iv) any other law relating to the data protection, security, or privacy of individuals that applies in the EU Area; or (v) any successor or amendments thereto (including, without limitation, implementation of the EU GDPR by Member States into their national law);

(g) "**Services**" means the services to be supplied by DashLoc to Customer or Customer's Affiliates pursuant to the Agreement; and

(h) **"Third Country**" means countries that, where required by applicable Data Protection Laws, have not received an adequacy decision from an applicable authority relating to cross-border data transfers of Personal Data, including regulators such as the European Commission, UK ICO, or Swiss FDPIC.

1.2. The terms "**Business**", "**Business Purpose**", "**commercial purpose**", "**Contractor**", "**Controller**", "**Data Subject**", "**Personal Data**", "**Personal Data Breach**", "**Process**", "**Processor**", "**Sell**", "**Service Provider**", "**Share**", "**Subprocessor**", "**Supervisory Authority**", and "**Third Party**" have the same meanings as described in applicable Data Protection Laws and cognate terms shall be construed accordingly.

1.3. Capitalized terms not otherwise defined in this Addendum shall have the meanings ascribed to them in the Agreement.

2. Roles of the Parties

2.1. The Parties acknowledge and agree that with regard to the Processing of Customer Personal Data, and as more fully described in **Annex 1** hereto, Customer acts as a Business or Controller, and DashLoc acts as a Service Provider or Processor. This Addendum shall apply solely to the Processing of Customer Personal Data by DashLoc acting as a Processor, Subprocessor, or Third Party (as specified in Annex 1).

2.2. The Parties expressly agree that Customer shall be solely responsible for ensuring timely communications to Customer's Affiliates or the relevant Controller(s) who receive the Services, insofar as such communications may be required or useful in light of applicable Data Protection Laws to enable Customer's Affiliates or the relevant Controller(s) to comply with such Laws.

3. Description and Purpose of Personal Data Processing

3.1. In **Annex 1** to this Addendum, the Parties have mutually set out their understanding of the subject matter and details of the Processing of the Customer Personal Data to be Processed by DashLoc pursuant to this Addendum. The Parties may make reasonable amendments to **Annex 1** on mutual written agreement and as reasonably necessary to meet those requirements. **Annex 1** does not create any obligation or rights for any Party.

3.2. The purpose of Processing under this Addendum is the provision of the Services pursuant to the Agreement and any Order Form(s).

4. Data Processing Terms

4.1. Customer shall comply with all applicable Data Protection Laws in connection with the performance of this Addendum and the Processing of Customer Personal Data. In connection with its access to and use of the Services, Customer shall Process Customer Personal Data within such Services and provide DashLoc with instructions in accordance with applicable Data Protection Laws. As between the Parties, Customer shall be solely responsible for compliance with applicable Data Protection Laws regarding the collection of and transfer to DashLoc of Customer Personal Data. Customer agrees not to provide DashLoc with any data concerning a natural person's health, religion or any special categories of data as defined in Article 9 of the

GDPR.

4.2. DashLoc shall comply with all applicable Data Protection Laws in the Processing of Customer Personal Data and DashLoc shall:

(a) Process the Customer Personal Data for the purposes of the Agreement and for the specific purposes in each case as set out in **Annex 1** to this Addendum and otherwise solely on the documented instructions of Customer, for the purposes of providing the Services and as otherwise necessary to perform its obligations under the Agreement. The Agreement, this Addendum, and Customer's use of the Services' features and functionality are Customer's written instructions to DashLoc in relation to Processing Customer Personal Data, including as follows:

(i) DashLoc shall use, retain, disclose, or otherwise Process Customer Personal Data only on behalf of Customer and for the specific business purpose of providing the Services and in accordance with Customer's instructions, including as described in the Agreement. DashLoc shall not Sell or Share Customer Personal Data, nor use, retain, disclose, or otherwise Process Customer Personal Data outside of its business relationship with Customer or for any other purpose (including DashLoc's commercial purpose) except as required or permitted by law. DashLoc shall immediately inform Customer (a) if DashLoc determines that it is no longer able to meet its obligations under Data Protection Laws or (b) if, in DashLoc's opinion, an instruction infringes applicable Data Protection Laws. Customer reserves the right to take reasonable and appropriate steps to ensure Graphite's Processing of Customer Personal Data is consistent with Customer's obligations under Data Protection Law and discontinue and remediate unauthorized use of Customer Personal Data;

(ii) DashLoc shall have rights to process Customer Personal Data solely (i) to the extent necessary to (a) perform the Business Purposes and its obligations under the Agreement; (b) operate, manage, test, maintain and enhance the Services including as part of its business operations; (c) to disclose aggregate statistics about the Services in a manner that prevents individual identification or re-identification of Customer Personal Data, including without limitation any individual device or individual person; and/or (d) protect the Services from a threat to the Services or Customer Personal Data; or (ii) if required by court order of a court or authorized governmental agency, provided that prior notice first be given to Customer; (iii) as otherwise expressly authorized by Customer;

(iii) DashLoc will not combine Customer Personal Data which DashLoc Processes on Customer's behalf, with Personal Data which it receives from or on behalf of another person or persons, or collects from its own interaction with individual, provided that Graphite may combine personal information to perform any Business Purpose permitted or required under the Agreement to perform the Services;

(b) implement and maintain measures designed to ensure that DashLoc personnel authorized to process the Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality unless disclosure is required by law or professional regulations;

(c) implement and maintain the technical and organizational measures set out in the Agreement, and, 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, implement and maintain any further commercially reasonable and appropriate administrative, technical, and organizational measures designed to ensure a level of security appropriate to the risk of the Processing of Customer Personal Data in accordance with Article 32 of the GDPR, and specifically:

(i) pseudonymization and encryption of Customer Personal Data;

(ii) ensuring ongoing confidentiality, integrity, availability and resilience of DashLoc's processing systems and services that process Customer Personal Data;

(iii) restoring availability and access to Customer Personal Data in a timely manner in the event of a physical or technical incident; and

(iv) regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing of the Customer Personal Data.

(d) Customer hereby agrees that DashLoc is generally authorized to engage and appoint Sub-processors**,** and specifically the Sub-processors listed in **Annex 2** hereto, subject to DashLoc's:

(i) notifying Customer at least thirty (30) calendar days in advance oof any intended changes or additions to its Sub-processors listed in **Annex 2** by emailing notice of the intended change to Customer;

(ii) including data protection obligations in its contract with each Sub-processor that are materially the same as those set out in this Addendum; and

(iii) remaining liable to Customer for any failure by each Sub-processor to fulfill its obligations in relation to the Processing of the Customer Personal Data.

In relation to any notice received under section 4.2(d)(i), Customer shall have a period of 30 (thirty) days from the date of the notice to inform DashLoc in writing of any reasonable objection on data protection grounds to the use of that Sub-processor. The parties will then, for a period of no more than 30 (thirty) days from the date of Customer's objection, work together in good faith to attempt to find a commercially reasonable solution for Customer which avoids the use of the objected-to Sub-processor. Where no such solution can be found, either Party may (notwithstanding anything to the contrary in the Agreement) terminate the relevant Services immediately on written notice to the other Party, without damages, penalty or indemnification whatsoever (but without prejudice to any fees incurred by Customer prior to termination);

(e) to the extent legally permissible, promptly notify Customer in case of any legally binding requests (i.e., disclosures required by law, court order, or subpoena) for disclosure of Customer Personal Data by DashLoc. In case if it is not legally binding then Customer Personal Data would not be disclosed and DashLoc will notify the Customer of such request rejection. A record of all legally binding disclosure requests relating to Customer Personal Data shall be maintained.

(f) to the extent legally permissible, promptly notify Customer of any communication from a Data Subject regarding the Processing of Customer Personal Data, or any other communication (including from a Supervisory Authority) relating to any obligation under the applicable Data Protection Laws in respect of the Customer Personal Data. DashLoc will not respond to any such request or complaint unless expressly authorized to do so by Customer or is otherwise required to respond under applicable Data Protection Laws. Taking into account the nature of the Processing, DashLoc will reasonably assist Customer (or the relevant Controller) by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of Customer's, Customer's Affiliates' or the relevant Controller(s)' obligation to respond to requests for exercising the data subject's rights laid down in Chapter Ill GDPR. Customer agrees to pay DashLoc for time and for out of pocket expenses incurred by DashLoc in connection with the performance of its obligations under this Section 4.2(e);

(g) upon DashLoc's becoming aware of a Personal Data Breach involving Customer Personal Data, notify

Customer without undue delay, of any Personal Data Breach involving Customer Personal Data, such notice to include, to the extent reasonably available to DashLoc, all timely information reasonably required by Customer (or the relevant Controller) to comply with its data breach reporting obligations under the applicable Data Protection Laws. DashLoc shall further take all such measures and actions as are necessary to remedy or mitigate the effects of such Security Incident and shall keep Customer reasonably informed of developments concerning Customer Personal Data;

(h) to the extent required by the applicable Data Protection Laws, provide reasonable assistance to Customer, Customer's Affiliates' or the relevant Controller(s)' with its obligations pursuant to Articles 32 to 36 of the GDPR taking into account the nature of the Processing and information available to DashLoc; Customer agrees to pay DashLoc for time and for out of pocket expenses incurred by DashLoc in connection with any assistance provided in connection with Articles 35 and 36 of the GDPR;

(i) cease Processing the Customer Personal Data upon the termination or expiry of the Agreement, and at option of Customer, Customer's Affiliates or the relevant Controller(s) either return or delete (including by ensuring such data is in non-readable format) all copies of the Customer Personal Data Processed by DashLoc, unless (and solely to the extent and for such period as) applicable law requires DashLoc to retain some or all of the Customer Personal Data. Any such Customer Personal Data retained shall remain subject to the obligations of confidentiality set forth in the Agreement; and

(j) DashLoc shall maintain the necessary records in support of demonstrating compliance with its obligations (as specified in the applicable contract) for the processing of Customer Personal Data carried out on behalf of the Customer.

(k) make available to Customer all information reasonably necessary to demonstrate compliance with this Addendum and allow for and contribute to audits, including inspections, by Customer, or an independent third party auditor mandated by Customer, provided that Customer gives DashLoc reasonable prior notice of its intention to audit, conducts its audit during DashLoc's normal business hours, and takes all reasonable measures to prevent unnecessary disruption to DashLoc's operations. For the purposes of demonstrating compliance with this Addendum under this Section 4.2(i), the Parties agree that in the first instance, once per year during the term of the Agreement (except if and when required by instruction of a competent Supervisory Authority or where Customer believes a further audit is necessary due to a Personal Data Breach concerning Customer Personal Data suffered by DashLoc), DashLoc will provide to Customer responses to cybersecurity and other assessments and only where Customer cannot establish DashLoc's compliance with this Addendum from DashLoc's responses shall Customer request to inspect DashLoc's processing operations. Customer agrees to pay DashLoc for time and for out of pocket expenses incurred by DashLoc in connection with assistance provided in connection with such audits, responses to cybersecurity and other assessments.

5. Restricted Transfers

5.1. The parties agree that when the transfer of Customer Personal Data from Customer and/or any of its Affiliates (as exporter) to DashLoc (as importer) is a Restricted Transfer and EU Area Law applies, the transfer shall be subject to the appropriate Controller to Processor SCCs, which shall be deemed incorporated into and form part of this Addendum as follows:

(a) In relation to Customer Personal Data that is protected by the EU GDPR and processed by DashLoc on behalf of and under the instruction of Customer, the EU SCCs will apply completed as follows:

(i) Module Two will apply (*controller to processor transfers*);

(ii) In Clause 7, the optional docking clause will apply;

(iii) In Clause 9, Option 2 will apply, and the time period for prior notice of sub-processor changes shall be as set out in Section 4.2(d) of this Addendum;

(iv) In Clause 11, the optional language will not apply;

(v) In Clause 17, Option 1 will apply, and the EU SCCs will be governed by Irish law;

(vi) In Clause 18(b), disputes shall be resolved before the courts of the Republic of Ireland;

(vii) Annex I of the EU SCCs shall be deemed completed with the information set out in Annex 1 to this Addendum; and

(viii) Annex II of the EU SCCs shall be deemed completed with the information set out in in Section 4 of Annex 1 to this Addendum.

(b) In relation to Customer Personal Data that is protected by the Swiss DPA, the EU SCCs shall apply in accordance with Section 5.1(a) of this Addendum, but with the following modifications:

(i) Any references in the EU SCCs to "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss DPA and the equivalent articles or sections therein;

(ii) Any 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;

(iii) Any references to the "competent supervisory authority" and "competent courts" shall be interpreted as references to the relevant data protection authority and courts in Switzerland; and

(iv) The Controller to Processor SCCs shall be governed by the laws of Switzerland and disputes shall be resolved before the competent Swiss Courts.

(c) In relation to Customer Personal Data that is protected by the UK GDPR, the EU SCCs shall apply in accordance with Section 5.1(a) of this Addendum, but as modified and interpreted by the Part 2: Mandatory Clauses of the UK Addendum, which shall be incorporated into and form an integral part of this Addendum. Any conflict between the terms of the EU SCCs and the UK Addendum shall be resolved in accordance with Section 10 and Section 11 of the UK Addendum. In addition, tables 1 to 3 in Part 1 of the UK Addendum shall be completed respectively with the information set out in Annex I of this Addendum, and table 4 in Part 1 of the UK Addendum shall be deemed completed by selecting both "Importer" and "Exporter".

5.2. DashLoc shall not participate in any other Restricted Transfers of Customer Personal Data (whether as an importer or an exporter of the Customer Personal Data) unless the Restricted Transfer is made in compliance with applicable Data Protection Law and pursuant to the relevant Standard Contractual Clauses implemented between the relevant exporter and importer of the Customer Personal Data, as necessary in order to comply with applicable Data Protection Law

6. Precedence

6.1. The provisions of this Addendum are supplemental to the provisions of the Agreement. In the event of any inconsistency between the provisions of this Addendum and the provisions of the Agreement, the provisions of this Addendum shall prevail. In the event that any provision of this Addendum and/or the Agreement

contradicts, directly or indirectly, the Controller to Processor SCCs, the Controller to Processor SCCs will control.

7. Indemnity

7.1. To the extent permissible by law, Customer shall (a) defend DashLoc and its Affiliates (collectively, "**Indemnified Parties**") from and against any and all claims, demands, suits, or proceedings made or brought against any of the Indemnified Parties by any third party (each, a "**Claim**"), and (b) indemnify and hold harmless the Indemnified Parties from and against any and all losses, damages, liabilities, fines and administrative fines, penalties, settlements, and costs and expenses of any kind (including, without limitation, reasonable legal, investigatory and consultancy fees and expenses) incurred or suffered by any of the Indemnified Parties, in each case arising from any breach by Customer of this Addendum or of its obligations under applicable Data Protection Laws. DashLoc may participate in the defense and/or settlement of a Claim under this Section 7.1 with counsel of its choosing at its own expense.

8. Severability

8.1. The Parties agree that, if any section or sub-section of this Addendum is held by any court or competent authority to be unlawful or unenforceable, it shall not invalidate or render unenforceable any other section of this Addendum.

9. Miscellaneous.

9.1. The Addendum considers the following and follows:

(a) Privacy by Design and default

(b) Achieving security of Processing

(c) Notification of breaches involving Customer Personal Data to the relevant Supervisory Authority

(d) Notification of breaches involving Customer Personal Data to Customer

(e) Conducting Privacy Impact Assessment where appropriate and required by applicable Data Protection Law

(f) Assurance of DashLoc's assistance by if prior consultations with relevant Supervisory Authorities are needed and required by applicable Data Protection Laws.

9.2. DashLoc shall comply with all statutory and regulatory requirements, ISO 27001:2013, ISO 27701:2019 and EU GDPR requirements.

9.3. In the event a Data Subject wishes to exercise its data subject rights under applicable Data Protection Law, including, but not limited to, a data subject's right of access, correction and/or erasure of its Personal Data in DashLoc's control, the Data Subjects can submit such request done by contacting DashLoc's Data Protection Officer (DPO) below. Also for raising concerns and/or any complaints related to the Customer Personal Data that can be done by contacting the Data Protection Officer below:

Name: Gaurav Kumar

Email ID: gaurav@dashloc.com

9.4. There are no Temporary files getting generated during processing.

Annex 1 to Data Protection Addendum

Description of Processing Activities for Customer Personal Data

This Annex includes certain details of the Processing of Customer Personal Data by DashLoc in connection with the Services.

1. **List of Parties**

Data Exporter

Name:	Customer (as defined in the Agreement)
Address:	As set forth in the relevant Order Form.
Contact person's name, position and contact details:	As set forth in the relevant Order Form.
Activities relevant to the data transferred under these Clauses:	Recipient of the Services provided by DashLoc in accordance with the Agreement.
Signature and date:	Signature and date are set out in the Agreement.
Role (controller/processor):	Controller

Data Importer

Name:	DashLoc
Address:	registered office at **No.44, Backary Portion 2nd Floor, Regal Building New Delhi G.P.O. New Delhi Central Delhi 110001**
Contact person's name, position and contact details:	**Gaurav Kumar, gaurav@dashloc.com, 08041485914**
Activities relevant to the data transferred under these Clauses:	Provision of the Services to the Customer in accordance with the Agreement.
Signature and date:	Signature and date are set out in the Agreement.
Role (controller/processor):	Processor

2. Competent Supervisory Authority

Identify the competent supervisory authority/ies in accordance (e.g. in accordance with Clause 13 SCCs)	As determined by application of Clause 13 of the EU SCCs.

3. Processing Information

Categories of data subjects whose personal data is transferred	Customer's authorized users of the Services
Categories of personal data transferred	Processed automatically by the Services: • Names • email IDs

Sensitive personal data transferred	None
Frequency of the transfer	Continuous
Nature of the processing Purpose of the data transfer and further processing	The nature of the processing is more fully described in the Agreement and accompanying order forms but will include the following basic processing activities: The provision of Services to Customer. In order to provide people data, DashLoc receives identifying Customer Personal Data to permit DashLoc to query, cleanse, standardize, enrich, (when required) send to additional data to feed providers, and to store the query information. The purpose of the transfer is to facilitate the performance of the Services more fully described in the Agreement and accompanying order forms.
For processing involving California consumers, please select the Business Purpose(s) for Processing Personal Data	☐ N/A ☐ Auditing related to counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards ☒ Helping to ensure security and integrity to the extent the use of the consumer's personal information is reasonably necessary and proportionate for these purposes ☒ Debugging to identify and repair errors that impair existing intended functionality. ☐Inc Short-term, transient use, including, but not limited to, nonpersonalized advertising shown as part of a consumer's current interaction with the business, provided that the consumer's personal information is not disclosed to another third party and is not used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction with the business ☒ Performing services on behalf of the business, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing storage, or providing similar services on behalf of the business. ☐ Providing advertising and marketing services, except for cross-context behavioral advertising, to the consumer provided that, for the purpose of advertising and marketing, a service provider or contractor shall not combine the personal information of opted-out consumers that the service provider or contractor

	receives from, or on behalf of, the business with personal information that the service provider or contractor receives from, or on behalf of, another person or persons or collects from its own interaction with consumers. ☒ Undertaking internal research for technological development and demonstration. ☒ Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business. ☒ To retain and employ another service provider or contractor as a subcontractor where the subcontractor meets the requirements for a service provider or contractor under CCPA. ☒ To build or improve the quality of the services it is providing to the business even if this Business Purpose is not specified in the written contract required by CCPA provided that Service Provider does not use the Customer Personal Data to perform Services on behalf of another person. ☒ To prevent, detect, or investigate data security incidents or protect against malicious, deceptive, fraudulent, or illegal activity, even if this Business Purpose is not specified in the written contract.
Period for which the personal data will be retained or criteria used to determine that period	The period for which the Customer Personal Data will be retained is more fully described in the Agreement, Addendum, and accompanying order forms.
Subprocessor transfers – subject matter, nature, and duration of processing	The subject matter, nature, and duration of the Processing more fully described in the Agreement, Addendum, and accompanying order forms.

4. Technical and Organisational Security Measures

Description of the technical and organisational security measures implemented by DashLoc as the data processor/data importer to ensure an appropriate level of security, taking into account the nature, scope, context, and purpose of the processing, and the risks for the rights and freedoms of natural persons.

4.1. **Security**

4.1.1. **Security Management System**.

(a) **Organization**. DashLoc designates qualified security personnel whose responsibilities include

development, implementation, and ongoing maintenance of the Information Security Program.

(b) **Policies**. Management reviews and supports all security related policies to ensure the security, availability, integrity and confidentiality of Customer Personal Data. These policies are updated at least once annually.

(c) **Assessments**. DashLoc engages a reputable independent third-party to perform risk assessments of all systems containing Customer Personal Data at least once annually.

(d) **Risk Treatment**. DashLoc maintains a formal and effective risk treatment program that includes penetration testing, vulnerability management and patch management to identify and protect against potential threats to the security, integrity or confidentiality of Customer Personal Data.

(e) **Vendor Management**. DashLoc maintains an effective vendor management program

(f) **Incident Management**. DashLoc reviews security incidents regularly, including effective determination of root cause and corrective action.

(g) **Standards**. DashLoc operates an information security management system that complies with the requirements of ISO/IEC 27001:2013 standard.

4.2. **Personnel Security**.

4.2.1. DashLoc personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. DashLoc conducts reasonably appropriate background checks on any employees who will have access to client data under this Agreement, including in relation to employment history and criminal records, to the extent legally permissible and in accordance with applicable local labor law, customary practice and statutory regulations.

4.2.2. Personnel are required to execute a confidentiality agreement in writing at the time of hire and to protect Customer Personal Data at all times. Personnel must acknowledge receipt of, and compliance with, DashLoc's confidentiality, privacy and security policies. Personnel are provided with privacy and security training on how to implement and comply with the Information Security Program. Personnel handling Customer Personal Data are required to complete additional requirements appropriate to their role (e.g., certifications). DashLoc's personnel will not process Customer Personal Data without authorization.

4.3. **Access Controls**

4.3.1. **Access Management**. DashLoc maintains a formal access management process for the request, review, approval and provisioning of all personnel with access to Customer Personal Data to limit access to Customer Personal Data and systems storing, accessing or transmitting Customer Personal Data to properly authorized persons having a need for such access. Access reviews are conducted periodically to ensure that only those personnel with access to Customer Personal Data still require it.

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

4.3.3. **Access Control and Privilege Management**. DashLoc's and Customer's administrators and end users must authenticate themselves via a Multi-Factor authentication system or via a single sign on system

in order to use the Services

4.3.4. **Internal Data Access Processes and Policies – Access Policy**. DashLoc's internal data access processes and policies are designed to protect against unauthorized access, use, disclosure, alteration or destruction of Customer Personal Data. DashLoc designs its systems to only allow authorized persons to access data they are authorized to access based on principles of "least privileged" and "need to know", and to prevent others who should not have access from obtaining access. DashLoc requires the use of unique user IDs, strong passwords, two factor authentication and carefully monitored access lists to minimize the potential for unauthorized account use. The granting or modification of access rights is based on: the authorized personnel's job responsibilities; job duty requirements necessary to perform authorized tasks; a need to know basis; and must be in accordance with DashLoc's internal data access policies and training. Approvals are managed by workflow tools that maintain audit records of all changes. Access to systems is logged to create an audit trail for accountability. Where passwords are employed for authentication (e.g., login to workstations), password policies follow industry standard practices. These standards include password complexity, password expiry, password lockout, restrictions on password reuse and re-prompt for password after a period of inactivity

4.4. **Data Center and Network Security**

4.4.1. **Data Centers.**

(a) **Infrastructure.** DashLoc has AWS as its data center.

(b) **Resiliency.** Multi Availability Zones are enabled on AWS and DashLoc conducts Backup Restoration Testing on regular basis to ensure resiliency.

(c) **Server Operating Systems.** DashLoc's servers are customized for the application environment and the servers have been hardened for the security of the Services. DashLoc employs a code review process to increase the security of the code used to provide the Services and enhance the security products in production environments.

(d) **Disaster Recovery**. DashLoc replicates data over multiple systems to help to protect against accidental destruction or loss. DashLoc has designed and regularly plans and tests its disaster recovery programs.

(e) **Security Logs.** DashLoc's systems have logging enabled to their respective system log facility in order to support the security audits, and monitor and detect actual and attempted attacks on, or intrusions into, DashLoc's systems.

(f) **Vulnerability Management.** DashLoc performs regular vulnerability scans on all infrastructure components of its production and development environment. Vulnerabilities are remediated on a risk basis, with Critical, High and Medium security patches for all components installed as soon as commercially possible.

4.4.2. **Networks and Transmission.**

(a) **Data Transmission**. Transmissions on production environment are transmitted via Internet standard protocols.

(b) **External Attack Surface**. AWS Security Group which is equivalent to virtual firewall is in place for Production environment on AWS.

(c) **Incident Response**. DashLoc maintains incident management policies and procedures, including detailed security incident escalation procedures. DashLoc monitors a variety of communication channels for security incidents, and DashLoc's security personnel will react promptly to suspected or known incidents, mitigate harmful effects of such security incidents, and document such security incidents and their outcomes.

(d) **Encryption Technologies**. DashLoc makes HTTPS encryption (also referred to as SSL or TLS) available for data in transit.

4.5. **Data Storage, Isolation, Authentication, and Destruction.** DashLoc stores data in a multi-tenant environment on AWS servers. Data, the Services database and file system architecture are replicated between multiple availability zones on AWS. DashLoc logically isolates the data of different customers. A central authentication system is used across all Services to increase uniform security of data. DashLoc ensures secure disposal of Client Data through the use of a series of data destruction processes.

Annex 2
DashLoc's Sub-processors

Name of Sub-processor	Description of Processing	Location of Sub-processor
Amazon Web Service	Running the Production environment including the Application and Databases	USA/India
Google Workspace	Email services	India