Data Processing Addendum

This Data Processing Addendum, including the selected modules of the Standard Contractual Clauses and Annexes (this "DPA"), is dated effective as of the effective date of the Agreement ("DPA Effective Date") and entered into between Vasion (as defined in the Agreement) and Customer.

This DPA forms a part of and is incorporated into the then-current and applicable Agreement between Customer and Vasion that governs the provision, use, and purchase of Vasion's Services described in the Agreement ("Services"). Capitalized terms used herein and not defined will have the meanings given to such terms in the Agreement.

1. DEFINITIONS

In this DPA, the following terms shall have the following meanings:

1.1. "Applicable Data Protection Law" means all international, federal, national, and state privacy and data protection laws that apply to the processing of Personal Data that is the subject matter of the Agreement (including, but not limited to, where applicable, European Data Protection Law and U.S. Data Protection Law (as defined below)).

1.2. "CCPA" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq*., as amended by the California Privacy Rights Act ("CPRA"), and its implementing regulations.

1.3. "Controller" means the entity that determines the purposes and means of the processing of Personal Data.

1.4. "Data Subject" means a natural person whose Personal Data is processed in the context of this DPA.

1.5. "European Data Protection Law" means: (i) on and after 25 May 2018, the Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation)("EU GDPR"); (ii) in respect of the United Kingdom the Data Protection Act 2018 and the 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) and the Swiss Federal Data Protection Act ("Swiss GDPR").

1.6. "Personal Data" shall have the meaning given to such term under Applicable Data Protection Law, but generally means any information relating to an identified or identifiable natural person where an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

1.7. "Processor" means an entity that is engaged to process Personal Data on behalf of the Controller, including, as applicable, any "service provider" as that term is defined by the CCPA.

1.8. "Security Incident" means a breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data (as defined in Section 2.1 below) transmitted, stored, or otherwise processed by Vasion or its Sub-Processors. "Security Incident" does not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, including unsuccessful login attempts, pings, port scans, denial of services attacks, and other network attacks on firewalls or networked systems.

1.9. "Standard Contractual Clauses" means: (i) where the E.U. 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 (E.U.) 2016/679 of the European Parliament and of the Council ("EU SCCs"); (ii) where the UK GDPR applies, the applicable standard data protection clauses adopted pursuant to Article 46(2)(c) or (d) of the UK GDPR ("UK SCCs"); and (iii) where the Swiss DPA applies, the applicable standard data protection clauses issued, approved or recognized by the Swiss Federal Data Protection and Information Commissioner ("Swiss SCCs").

1.10. "Sub-Processor" means an entity engaged by the Processor to process Customer Personal Data on behalf of, and under the instructions of, the Controller in connection with the provision of the Service. Sub-Processors exclude employees, consultants, or independent contractors of Vasion where such individual performs services equivalent to those performed by an employee.

1.11. "U.S. Data Protection Law" means the data protection or privacy laws and regulations applicable to the processing of Personal Data in force within the United States, including, but not limited to, (i) the CCPA, (ii) the Virginia Consumer Data Protection Act ("VCDPA"), (iii) once in effect, the Colorado Privacy Act, Connecticut Act Concerning Personal Data Privacy and Online Monitoring, Utah Privacy Act, and (iv) any rules or regulations implementing any of the foregoing.

2. GENERAL DATA PROCESSING REQUIREMENTS

2.1 **Relationship of the parties**. As between the parties and for the purposes of this DPA, Customer is the Controller, with respect to E.U. Data Protection Law and VCDPA, and a "business" with respect to CCPA, of the Personal Data that is included in Customer Data ("Customer Personal Data") and appoints Vasion as a Processor, with respect to E.U. Data Protection Law and VCDPA, and a "service provider" with respect to CCPA, to process Customer Personal Data on behalf of Customer.

2.2 **Responsibilities of Vasion.** Vasion will not sell Customer Personal Data as the term "sell" is defined by the CCPA. Vasion will not disclose or transfer Customer Personal Data to other parties that would constitute "selling," as the term is defined by the CCPA. Customer shall comply with its obligations under Applicable Data Protection Law, including, but not limited to, providing notice to Data Subjects and obtaining Data Subjects' consent for processing of Data Subjects' Personal Data, where required. Vasion represents that its use of the Service will: (i) not violate the rights of any Data Subject that has opted-out from sales or other disclosures of Customer Personal Data to the extent applicable under the CCPA; and (ii) not violate the rights of any Data Subject that has not opted into the processing of sensitive personal data to the extent applicable under the VCDPA.

2.3 **Responsibilities of Customer**. Customer, as a Controller or as a "business," (as defined by the CCPA) is responsible for: (i) the accuracy, quality, and legality of the Customer Personal Data; (ii) how Customer acquired such data; (iii) the instructions Customer provides to Vasion regarding the processing of Customer Personal Data; (iv) providing all legally required notices to individuals and obtaining all legally required consents which may be necessary for Vasion to process Customer Personal Data; (v) ensuring that Customer's processing instructions are lawful and do not violate Applicable Data Protection Laws; and (vi) ensuring that Customer Personal Data is provided to Vasion for a valid "Business Purpose," as defined in the CCPA. Customer will not provide or make available to Vasion any Customer Personal Data in violation of the Agreement or provide any Customer Personal Data that is inappropriate for the nature of the Services.

2.4 **Processing instructions; Purpose limitation.** Vasion shall process Customer Personal Data as a Processor in accordance with the documented instructions of Customer (including those in this DPA and the Agreement) or with Customer's written instructions and only for the following purposes: (i) as necessary to perform the Services for Customer under the Agreement; (ii) to perform any steps necessary for the performance of the Agreement; (iii) any processing initiated by an Authorized User in their use of the Service; and (iv) to comply with other reasonable, lawful instructions provided by Customer (e.g., via email, phone, support tickets, or online tool). Customer shall only give lawful instructions to Vasion that comply with Applicable Data Protection Law. Annex A, attached hereto, includes certain details of the processing of Customer Personal Data, as required under Applicable Data Protection Law.

2.5 **Confidentiality of processing**. Vasion shall ensure that any person that it authorizes to process Customer Personal Data (including Vasion's staff, agents, and subcontractors) shall be subject to a duty of confidentiality (whether a contractual duty or a statutory duty) and shall not permit any person to process Customer Personal Data who is not under such a duty of confidentiality.

2.6 **Security standards**. Vasion shall implement appropriate technical and organizational measures pursuant applicable privacy laws, intended to protect Customer Personal Data from: (i) accidental or unlawful destruction; and (ii) loss, alteration, unauthorized disclosure of, or access to Customer Personal Data. At a minimum, such measures shall include the security measures identified in Annex B ("Security Measures"). Vasion may update or modify them from time to time provided that such updates and modifications do not result in the degradation of the overall security of the measures implemented by Vasion. Customer is responsible for reviewing the information Vasion makes available regarding its TOMS and data security, including its Audit Reports, and for making an independent determination as to whether the Services meet the Customer's requirements and legal obligations, including its legal obligations under the Applicable Data Protection Law.

3. SUB-PROCESSORS AND SUBCONTRACTING

3.1 Subject to the terms and conditions set forth in this DPA, Customer generally authorizes Vasion to continue to use and disclose Customer Personal Data to Sub-Processors engaged by Vasion in the context of providing the Services and processing activities. Customer approves the use of Sub-Processors described in Annex C. Vasion shall be liable for a breach of Vasion's obligations under this DPA that is caused by an act, error, or omission of Vasion's Sub-Processors, subject to the Limitation of Liability in Section 10 of the Agreement.

3.2 Vasion shall not subcontract any processing of Customer Personal Data to a third-party Sub-Processor unless: (i) such Sub-Processor is subject to an agreement with Vasion that contains data protection terms not less protective as those provided for by this DPA with respect to the protection of Customer Personal Data to the extent applicable to the nature of the service provided by such Sub-Processor; and (ii) Vasion provides

Customer prior notice (where notice will be provided by Vasion by email to Customer's Service account administrator or by an in-product notification within the Service) of the addition or replacement of such Sub-Processor (including the details of the processing it performs or will perform, and the location of such processing) before authorizing any new Sub-Processor(s) to process Customer Personal Data in connection with the provision of the applicable Service. Notwithstanding the foregoing, in the event of an emergency concerning Service availability or security, Vasion is not required to provide prior notice but shall provide notification within seven (7) business days following the change in Sub-Processor.

3.3 Provided that (i) a new Sub-Processor sub-processes Customer's Personal Data and (ii) Customer can reasonably demonstrate that such new Sub-Processor is unable to Process Customer's Personal Data in compliance with this DPA or Applicable Data Protection Law, if Customer wishes to object to such new Sub-Processor, Customer will notify Vasion within Fifteen (15) calendar days of receipt of Vasion's notice of a new Sub-Processor. Customer's objection should be sent to legalteam@vasion.com and explain the reasonable grounds for the objection based on (ii) above. If Customer objects to Vasion's appointment of a third party Sub-Processor on reasonable grounds and, within thirty (30) days of receipt of the notice of objection from Customer, Vasion is unable to adequately address the reasonable grounds (e.g., make available to Customer a reasonable change to Customer's configuration or use of the Service to avoid the processing of Customer Personal Data by the objected-to new Sub-Processor without unreasonably burdening Customer), then Vasion will, in its discretion, 1) not engage the Sub-Processor, or 2) suspend or terminate Customer's subscription to the specific elements of the Service impacted by the change [without penalty]. If Customer does not object to a Sub-Processor within fifteen (15) days of Vasion's notice as described in this Section 3, then the Sub-Processor will be deemed accepted by Customer.

4. INTERNATIONAL TRANSFERS OF DATA. To perform the Services for Customer under the Agreement, Vasion may transfer Customer Personal Data to countries other than the country in which the data were originally collected, including, without limitation, the United States. Vasion will ensure that such transfers are made in compliance with Applicable Data Protection Law and this DPA. Customer authorizes such cross-border Personal Data transfers and represents, warrants, and covenants that Customer will comply with any requirements under Applicable Data Protection Law regarding such Personal Data transfers. For such cross-border Personal Data transfers subject to Applicable Data Protection Law, Vasion and Customer agree to be bound by: (i) in the case of GDPR, the EU SCCs then-current and applicable module and terms of the Standard Contractual Clauses published by the European Commission; (ii) in the case of UK GDPR, the UK SCCs; and (iii) in the case of Swiss GDPR, the Swiss SCCs. In connection with the Standard Contractual Clauses referred to in (i) and (ii) of this Section 4, the parties agree to the following, as applicable:

4.1 With respect to Customer Personal Data processed by Vasion pursuant to Section 2.3.1:

a) Module Two of the EU SCCs will apply;

b) in Clause 7, the optional docking clause will apply;

c) in Clause 9, the Option 2 will apply;

d) in Clause 11, the optional language will not apply;

e) in Clause 17, Option 1 will apply, and the Standard Contractual Clauses will be governed by Irish law;

f) in Clause 18(b), disputes shall be resolved before the courts of Ireland;

g) Annex 1 will be deemed completed with the information set out in Annex A (Details of Processing) of this DPA;

h) Annex 2 (Security Measures) will be deemed completed with the information set out in Annex B of this DPA; and

i) Annex 3 (Sub-Processors) will be deemed completed with the information set out in Section 3 of this DPA.

4.2 With respect to Personal Data subject to UK GDPR, the UK SCCs will apply and:

a) the EU SCCs will also apply to transfers of Personal Data; and

b) Table 1 to 3 of the UK SCCs will be deemed completed with the relevant information from the EU SCCs completed as set forth in Sections 4.1 and 4.2 above and the option "neither party" is checked in Table 4. The start date of the UK SCCs in Table 1 will be the DPA Effective Date.

4.3 With respect to Personal Data subject to Swiss GDPR, the Swiss SCCs will apply and:

a) the EU SCCs will apply and any references in the EU SCCs to "Directive 95/46/EC" or "Regulation (EU) 2016/679" will be interpreted as references to the Swiss SCCs;

b) references to "EU," "Union," "Member State," and "Member State Law" will be interpreted as references to "Switzerland' and 'Swiss law,' as the case may be; and

c) references to the “competent supervisory authority” and “competent courts" shall be interpreted as references to the FDIPC 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 SCCs, in which event the Swiss SCCs shall instead be incorporated by reference and form an integral part of this DPA 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 A and Annex B to this DPA.

4.4 To the extent Vasion adopts an alternative data export mechanism (including any new version of or successor to the Standard Contractual Clauses adopted pursuant to Applicable Data Protection Laws) for the transfer of Personal Data (“**Alternative Transfer Mechanism**”), the Alternative Transfer Mechanism will automatically apply instead of any applicable transfer mechanism described in this DPA (but only to the extent such Alternative Transfer Mechanism complies with Applicable Data Protection Laws applicable to the European Economic Area and extends to territories to which Customer Personal Data is transferred).

5. COOPERATION AND INDIVIDUALS’ RIGHTS. Taking into account the nature of the processing and the information available, Vasion shall provide all reasonable and timely assistance to enable Customer to respond to: (i) any request from a Data Subject to exercise any of its rights under Applicable Data Protection Law (including its rights of access, correction, objection, erasure, and data portability, as applicable); and (ii) any other correspondence, inquiry, or complaint received from a regulator or public authority, Data Subject, or another third party, in connection with the processing of Customer Personal Data. If any such communication is made directly to Vasion, Vasion shall promptly and without undue delay (and in any event, no later than within forty-eight (48) hours of receiving such communication) provide Customer with full details of the same and shall not respond to the communication unless specifically required by law or authorized by Customer. To the extent permitted by Applicable Data Protection Law, Customer shall be responsible for any reasonable costs arising from Vasion’s or its Sub-Processor’s provision of such assistance.

6. DATA PROTECTION IMPACT ASSESSMENT. Taking into account the nature of the processing and the information available to Vasion, Vasion shall provide Customer with reasonable and timely assistance with any reasonable data protection impact assessments and, where necessary, consultations with data protection authorities.

7. SECURITY INCIDENT

7.1 Upon becoming aware of a Security Incident affecting Customer Personal Data, Vasion shall: (a) inform Customer without undue delay and in any event, no later than the earlier of, (i) within forty-eight (48) hours after confirming a Security Incident affected the data, and (ii) the time period required by Applicable Data Protection Laws; and (b) provide sufficient available information and cooperation to enable Customer to fulfil its data breach reporting obligations under (and in accordance with the timescales required by) Applicable Data Protection Law.

7.2 Vasion shall further take such measures and actions as are necessary to contain, investigate, remedy, and mitigate the Security Incident and shall keep Customer informed of all material developments in connection with the Security Incident. Vasion shall not notify any Data Subjects that a Security Incident specifically affects Customer and Customer Personal Data unless and to the extent that: (a) Customer has agreed to such notification, or (b) such notification is required to be made by Vasion under Applicable Data Protection Laws. Customer is responsible for its secure use of the Services, including, but not limited to, securing its account authentication credentials and protecting the security of data transmitted via the systems the Customer administers and maintains (i.e., email encryption).

8. DELETION OR RETURN OF DATA. During the term of the Agreement, Customer may access, export, or delete Customer Personal Data using the features included with the Services or by contacting Vasion for assistance as needed. Upon termination or expiry of the Agreement or upon the Customer’s written request, Vasion shall (at Customer's election and in accordance with the terms of Annex B and the Agreement) delete or return all Customer Personal Data, including copies, in its possession or control. This requirement shall not apply to the extent that Vasion is required by Applicable Data Protection Laws to retain some or all Customer Personal Data, in which event Vasion shall isolate and protect such data from any further processing except to the extent required by such law.

9. AUDIT RIGHTS AND REPORTS

9.1 Vasion will conduct an annual third-party audit to attest to the ISO 27001 and/or SOC 2 Type II framework (or equivalent or successor attestations or certifications). Such audit will result in the generation of a summary report, which Vasion will make available to Customer upon request, in addition to such other information regarding Vasion’s information security and privacy practices as Customer may reasonably request (together, “**Reports**”). All Reports are Vasion’s Confidential Information.

9.2 Solely to the extent required to comply with Applicable Data Protection Law, and to the extent the Reports do not satisfy Applicable Data Protection Law, Customer may audit (including by an independent third-party engaged by Customer who is not a competitor or Vasion and who must enter into a non-disclosure agreement with Vasion) Vasion's compliance with this DPA as it applies to Customer's Personal Data. In the case of such audit, subject to the terms of this DPA, the parties agree that: (a) Vasion shall make available all such information, systems, and staff reasonably necessary to allow Customer to conduct such audit; (b) Customer shall not exercise its audit rights more than once per calendar year except following a Security Incident or following a required instruction by a regulator or public authority; (c) Customer shall give Vasion at least forty-five (45) days prior written notice of its intention to audit pursuant to this DPA; (d) Customer shall conduct its audit during Vasion's normal business hours, and take all reasonable measures to prevent unnecessary disruption to the Services, Vasion's operations, and to ensure the protection of the data (which may include Personal Data) of Vasion's employees, contractors, suppliers, or other users or customers; (e) be limited in scope to matters reasonably required for Customer to assess Vasion's compliance with this DPA and the parties' compliance with Applicable Data Protection Law to the extent that they apply to Customer's Personal Data, and the parties shall mutually agree in advance on the date, scope, duration, and security and confidentiality controls applicable to an audit; (f) cover only facilities directly controlled by Vasion (unless otherwise agreed by the parties and any applicable Sub-Processors); (g) restrict findings to Customer Personal Data only; and (h) Customer and its auditors must treat any audit findings and results as Vasion's Confidential Information to the fullest extent permitted by Applicable Data Protection Laws.

9.3 Customer understands and agrees that its right to audit a Sub-Processor's compliance with this DPA will be subject to the audit provisions in the data processing terms between Vasion and such Sub-Processor, and that Customer may be required to execute a non-disclosure agreement and other related terms directly with such Sub-Processor to receive access to Sub-Processor's reports and policies.

9.4 Customer shall reimburse Vasion for all costs and expenses in connection with an audit carried out by Customer under this DPA, except that Vasion will provide Customer the Reports at no cost.

9.5 Customer must promptly advise Vasion of any non-compliance discovered as a result of an audit.

9.6 Customer agrees that any of its audit rights set out in the Standard Contractual Clauses and other Applicable Data Protection Law shall be subject to, and carried out in accordance with, the terms of this Section 9.

10. **COMPLIANCE WITH APPLICABLE LAWS**

10.1 Vasion will process Customer Personal Data in accordance with this DPA and Applicable Data Protection Laws applicable to its role under this DPA. Vasion is not responsible for complying with Applicable Data Protection Laws uniquely applicable to the Customer by virtue of its business or industry. Vasion will promptly inform Customer if it becomes aware that Customer's processing instructions infringe Applicable Data Protection Laws.

10.2 With respect to the CCPA, Vasion will: (i) comply with sections of the CCPA applicable to "service providers" as defined by the CCPA; (ii) process Customer Personal Data solely to provide the Services to Customer, consistent with Section 1798.140(e)(5) of the CCPA; and (iii) not sell Customer Personal Data, or retain, use, or disclose Customer Personal Data for any purposes other than to perform the Service or as otherwise permitted under Agreement or this DPA.

10.3 With respect to the VCDPA, Vasion will: (i) comply with sections of the VCDPA applicable to "processors" as defined by the VCDPA; and (ii) process Customer Personal Data solely to provide the Services to Customer.

11. COSTS ALLOCATION AND LIABILITY

11.1 Each party will bear its own costs of the investigation, remediation, mitigation, and other related costs to the extent a Security Incident is caused by such party.

11.2 Each party will bear its own costs of any fines, penalties, damages, or other related amounts imposed by an authorized regulatory body, governmental agency, or court of competent jurisdiction to the extent arising from such party's breach of its obligations under this DPA.

11.3 To the maximum extent allowed under Applicable Data Protection Law and other applicable law, each party's liability under this DPA will be subject to Section 10 (Limitation of Liability) of the Agreement.

11.4 Vasion shall not be liable for the damage caused by a Processing and/or in case of non-compliance with the Applicable Data Protection Law, as a result of a Processing resulting in an administrative fine issued by Supervisory Authority or a court against Customer unless such damage or non-compliance directly results from:

11.4.1 Acts of Vasion beyond or contrary to Customer's written instructions;

11.4.2 Failure of Vasion's employees to comply with their applicable confidentiality obligations; or

11.4.3 Partial or total non-performance of the TOMs as set out in the Agreement.

12. MISCELLANOUS PROVISIONS

12.1 The obligations placed upon Vasion under this DPA shall survive so long as Vasion or its Sub-Processors process Customer Personal Data on behalf of Customer. The parties agree that this DPA will replace any existing data processing agreement the parties may have previously entered into in connection with the Services. Any claims against Vasion or its Affiliates under this DPA may only be brought by the Customer entity that is a contracting party to the Agreement. In no event shall this DPA or any party restrict or limit the rights of any Data Subject or of any competent supervisory authority.

12.2 The parties agree that this DPA applies to Vasion's Processing of Customer Personal Data under the Agreement solely to the extent such processing is subject to Applicable Data Protection Laws. Other than as required by the Standard Contractual Clauses, this DPA is governed by the governing law set forth in the Agreement unless otherwise required by Applicable Data Protection Laws.

12.3 Except for the changes made by this DPA, the Agreement continues to govern the provision and use of the Service and remains unchanged and in full force and effect (including, for avoidance of doubt, the Limitation of Liability, Section 10 of the Agreement). With the exception of Sections 9 and 10 of the Agreement, if there is any direct conflict between a provision in this DPA and a provision in the Agreement, the provision in this DPA shall prevail solely to the extent of that conflict only.

12.4 Other than as required by the Standard Contractual Clauses, this DPA does not confer any third-party beneficiary rights; it is intended for the benefit of the parties hereto, respective permitted successors, and assigns only, and is not for the benefit of, nor may any provision hereof be enforced by, any other person.

12.5 Other than as required by the Standard Contractual Clauses, the dispute mechanisms, including those related to venue and jurisdiction, set forth in the Agreement govern any dispute pertaining to this DPA.

12.6 Vasion may update the terms of this DPA from time to time. The then-current terms of this Addendum are available at vasion.com/legal/.

This DPA is accepted and agreed to by the parties effective as of the Agreement Effective Date.

ANNEX A

DETAILS OF PROCESSING OF PERSONAL DATA

(This Annex only applies to the Vasion Automate Platform and is not applicable to Vasion Automate Pro)

This Annex A includes certain details of the processing of Personal Data as required by the Standard Contractual Clauses and Article 28(3) GDPR. The parties agree that this Annex forms a part of the Standard Contractual Clauses.

A. List of Parties

Data exporter(s): Customer

Role: Controller or Processor (if processing contracts on behalf of an affiliate of Customer)

Contact Information: As outlined in the Agreement or provided by Customer in writing

Data importer(s): Vasion, Inc.

Role: Processor for purposes of Section 2.3.1 and Controller for purpose of Section 2.3.2

Contact Information: As outlined in the Agreement

B. Description of Transfer

The description of the transfer will differ depending on which application/product is being used, see below for further details:

(i) **Subject matter and duration of the processing of Data:**

VASION PRINT AND ON-PREMISE OFFERINGS: The Data Exporter has contracted with the Data Importer for certain software services. In its use of the software services the Data Exporter will upload certain personal data into the software's database which will be stored on servers in the United States unless the Data Exporter is located in the EEA, Canada, or Australia, in which case the data will be stored on servers in the EEA, Canada, or Australia respectively. The data may be accessed, on the Data Exporter's request, by the Data Importer in order to provide technical support services. The personal data will be processed for the duration of the contract for software services and for a further period of sixty (60) days to allow appropriate time for deletion and any requested return of the data to the Data Exporter.

VASION SIGNATURE, CAPTURE, FORMS, WORKFLOW, and STORAGE: The Data Exporter has contracted with the Data Importer for certain software services. In its use of the software services the Data Exporter will upload certain personal data into the software's database which will be stored on servers in the United States unless the Data Exporter is located in the United Kingdom or the EEA in which case the data will be stored on servers in the EEA. The data may be accessed, on the Data Exporter's request, by the Data Importer in order to provide technical support services. The personal data will be processed for the duration of the contract for software services and for a further period of sixty (60) days to allow appropriate time for deletion and any requested return of the data to the Data Exporter.

(ii) **The nature and purpose of the processing of Data:**

VASION PRINT AND ON-PREMISE OFFERINGS:

Nature of the processing:

The print management product uses any data including personal data that data exporter uploads to its services and products. The Data Importer does not access any personal data uploaded, except where it is necessary to provide technical support to the Data Exporter at the Data Exporter's request.

The Personal Data transferred to or accessed by the data importer will be used only for the purposes of providing the Services to the data exporter as described in further detail in the Agreement and this DPA. To this end, Personal Data may be accessed, processed, or disclosed as necessary by the data importer's duly authorised staff or Sub-Processors, strictly for the purpose of providing Services to the data exporter and in accordance with the data exporter's instructions set out in the Agreement and this DPA.

Vasion's Services (offered as a SaaS solution or an on-premise solution) performs two services that involve personal data.

1. Active Directory: A Vasion customer can establish an Active Directory within the Vasion Print software that identifies authorized users for a specific printer along with what manner the authorized user may use the printer. (i.e. printing in color or black only). The customer controls the information needed to run such authorizations (e.g. username, pin number, ID number, etc.)
2. Print Job Auditing and Reporting

The software provides the customer with the following information via a print report:

- Quantity of pages each department prints weekly, monthly, or quarterly;
- usage of any given printer to determine if a printer can be phased out;
- Actual cost of printing- itemized by department, location or printer;
- Identification of users;
- Notification of when a user prints a document labelled as “classified’;
- Overall printer usage data and printer consolidation guidance;
- Monitoring and reporting of all USB printing

3. *Off-Network Printing and Off-Network Cloud Print (“Off-Network Printing”): Allows user with internet access, from any location, to send print jobs to a printer located behind the company firewall without a VPN or special firewall rules. The print job is received by an external gateway and an internal routing service opens a new connection and downloads and delivers the print job to the designated printer. Print jobs are encrypted at their origination point and routed through the Vasion Print gateway service to their destination printer. The Data Importer does not retain or store the print job.
4. *Simplified Scanning: Users scan a physical document on a printer with the Vasion control panel application installed and send the document to a cloud storage location of the user’s choice or they may email the document to themselves or others as an email attachment. Vasion does not retain or store the scan job.

Purpose(s) of the data transfer and further processing:

For the on-premise solution, the Vasion software is installed behind the Customer’s firewall and Vasion does not have access to the customer’s network unless granted access during a product support request. For the SaaS solution, a client is installed locally that communicates with the Vasion product hosted in Amazon Web Services which customers may elect to be stored on servers in the United States, or in the EEA . Although a customer may elect to store data on servers in the EEA, for purposes of software development and support, a limited number of Vasion production engineers based in the United States may have access to data stored within servers in the EEA.

VASION AUTOMATE SIGNATURE, CAPTURE, FORMS, WORKFLOW, and STORAGE:

Nature of the processing:

The personal data processed will be subject to the following basic processing activities:

The Data Exporter processes any data including personal data that Data Exporter or its Users upload to the product. The Data Importer does not access any personal data except where it is necessary for Vasion to provide technical support to the Data Exporter at the Data Exporter’s request. Vasion merely offers technologies that its customers can use to store, retrieve, archive and share their data.

The Personal Data transferred to or accessed by the Data Importer will be used only for the purposes of providing the Services to the data exporter as described in further detail in the Agreement and this DPA. To this end, Personal Data may be accessed, processed, or disclosed as necessary by the Data Importer’s duly authorised staff or Sub-Processors, strictly for the purpose of providing Services to the data exporter and in accordance with the data exporter’s instructions set out in the Agreement and this DPA.

Data Exporter warrants to the Data Importer that where consent must be obtained to process the personal data, it has obtained such consent and that it has fully complied with its obligations in this regard.

Purpose(s) of the data transfer and further processing:

The Data Exporter and/ or its affiliate(s) have contracted with the Data Importer for a licence to use the Vasion product. In its use of the product the Data Exporter will upload content which may include personal data into the product which will be stored on servers according to where the Data Exporter is located. In accordance with the settings selected by the Data Exporter and its users, solely at their discretion, the Data Importer will permit the content including any personal data to be retrieved by the Data Exporter’s users from (i) the product and (ii) via elected third party products and services. The Data Importer does not have access to the content, including any personal data, unless access is required for the provision of technical services.

(iii) **Frequency of the Transfer:**

VASION PRINT AND ON-PREMISE OFFERINGS:: Continuous for the duration of the Agreement

VASION SIGNATURE, CAPTURE, FORMS, WORKFLOW, and STORAGE: Continuous for the duration of the Agreement.

(iv) **The categories of Personal Data to be transferred:**

VASION PRINT AND ON-PREMISE OFFERINGS: First name, last name, email address, title of print job, username and password.

*For the Off-Network printing and the Simplified Scanning functionalities, the Data Importer will process the actual print and scan jobs. The category of personal data contained in the print job or scan job shall be solely at the discretion of the Data Exporter.

VASION SIGNATURE, CAPTURE, FORMS, WORKFLOW, and STORAGE: The personal data transferred may concern the following categories of data: first name, last name, email address, title of printed document, username and password, IP addresses, email senders and recipients, and any other categories of personal data that maybe contained within the content uploaded to the Vasion product, solely at the discretion and control of the Data Exporter or its Users

(v) **The categories of Data Subject to whom the Data relates:**

VASION PRINT AND ON-PREMISE OFFERINGS: The personal data processed that may be transferred concerns the following categories of data subjects: Users of the Vasion application which may include employees and other personnel of the Data Exporter or of the customers of the Data Exporter, solely at the control and discretion of the Data Exporter or its Users.

*For the Off-Network Printing and Simplified Scanning functionalities, the personal data concerns Users of the Vasion application which may include personnel of the Data Exporter, Customers of the Data Exporter or any other individual whose personal data is contained within the content of the print job or scan job, always solely at the control and discretion of the Data Exporter and its Users.

VASION SIGNATURE, CAPTURE, FORMS, WORKFLOW, and STORAGE: The personal data processed which may be transferred concerns the following categories of data subjects: Users of the Vasion product which may include employees and other personnel of the Data Exporter or of the customers of the Data Exporter, any other individual whose personal data is contained within the content uploaded to Vasion, always solely at the control and discretion of the Data Exporter or its Users.

(vi) The obligations and rights of Customer:

The obligations and rights of Customer are set out in the Agreement and this DPA.

(vii) **Special categories of data (if appropriate):**

VASION PRINT AND ON-PREMISE OFFERINGS: The personal data processed that may be transferred would not normally include any special categories of data, but data exporter is in control in this regard. Data Exporter warrants to the Data Importer that where such consent must be obtained it has done so and that it has fully complied with its obligations in this regard.

For the Pull Printing functionality, the software will capture and store the title of a document which will be produced in print reports accessible to the Customer's IT personnel. The title of printed documents which may be reported (and stored) will be the title of the document as transmitted to the printer to be printed. This title may therefore contain special category data or personal data belonging to the data subject for which the data exporter may need to satisfy itself that it has obtained the express consent of the data subject to transfer in order to comply with its legal obligations under the General Data Protection Regulation 2016/679 (GDPR). The controller is in control and may turn this function on or off as it sees fit.

If controller turns this function off, the Pull Printing mode within software will capture and temporarily store the title of a document which will be encrypted and not accessible to the Customer's IT personnel and will be temporarily stored until released by the transmitter of the document or for a period of time elected by the Controller until automatic expiry.

For Off-Network Print and Simplified Scanning functionalities, the personal data processed may be any category of special data that is contained within the print job or scan solely at the discretion and control of the Data Exporter and its Users.

VASION SIGNATURE, CAPTURE, FORMS, WORKFLOW, and STORAGE: The personal data processed may contain the following special categories of data: any category of special data that may be contained within the content uploaded to the Vasion Services, solely at the discretion and control of the Data Exporter or its Users.

(viii) **The period for which the personal data will be retained:**

VASION PRINT AND ON-PREMISE OFFERINGS: The personal data will be processed for the duration of the contract for software services and for a further period of sixty (60) days to allow appropriate time for deletion and any requested return of the data to the Data Exporter. All back up, archived personal data will be permanently deleted after six (6) months from the termination of software services.

VASION SIGNATURE, CAPTURE, FORMS, WORKFLOW, and STORAGE: The personal data will be processed for the duration of the contract for software services and for a further period of sixty (60) days to allow appropriate time for deletion and any requested return of the data to the Data Exporter. All back up,

archived personal data will be permanently deleted after six (6) months from the termination of software services.

ANNEX B

TECHNICAL AND ORGANISATIONAL SECURITY MEASURES APPLICABLE FOR THE VASION AUTOMATE PLATFORM INCLUDING PRINT, SIGNATURE, CAPTURE, FORMS, WORKFLOW, AND STORAGE

(*This Annex only applies to the Vasion Automate Platform and is not applicable to Vasion Automate Pro)

The Vasion Automate Platform application is built and resides in Amazon Web Services (AWS) or MicroSoft Azure, at the discretion of the Customer. Details of physical security implementation for AWS and MicroSoft Azure are found both at www.infrastructure.aws, https://aws.amazon.com/compliance/data-center/controls/ or https://learn.microsoft.com/en-us/azure/security/fundamentals/physical-security

For the Vasion Automate Platform, Vasion follows the ISO 27001 framework for governance and operations. The Vasion Automate Platform is ISO 27001 and SOC 2 Type II certified.

1. System Access Control:

Vasion prevents unauthorized access to data processing systems as follows:

- Supports role-based access control (RBAC) for system administrators. Multi-factor authentication is required to access the production environment containing Customer Data,
- Ensures that all computers accessing Customer Data (this includes remote access) are password protected after boot sequences and have encrypted disks,
- Has dedicated user IDs for authentication against systems user management for every individual,
- Assigns individual user passwords for authentication,
- Ensures that the access control is supported by an authentication system,
- Only grants system access to Vasion's authorized personnel and/or to permitted employees of Vasion's subcontractors and strictly limits such persons' access to applications which process personal data as required for those persons to fulfil their function,
- Implements a password policy that prohibits the sharing of passwords, outlines processes after a disclosure of a password and requires the regular change of passwords,
- Ensures that passwords are always stored in encrypted form,
- Has a proper procedure to deactivate user accounts, when user leaves company or function, and
- Has a proper process to adjust administrator permissions when an administrator leaves company or function.

2. Processing of Personal Data:

Vasion protects Customer personal data it processes or stores in the Services it provides to Customers, as follows:

- Persons entitled to use data processing systems shall gain access only to the data to which they have a right of access, and personal data will not be copied, modified or removed without authorization in the course of processing. Including, without limitation, Vasion:
  - Restricts access to files and programs based on a "need-to-know-basis",
  - Only grants access to Vasion personnel and assigns minimal permissions to access data as needed to fulfil their function.
- The responsibilities for the processing of personal data are clearly described (controller, processor, sub-processor, etc.).
- Vasion requires its employees and subcontractors (if applicable) to maintain confidentiality with respect to personal data and other confidential information of which they become aware in the course of providing services.
- Applicable Vasion employees receive appropriate privacy and data protection training to the extent that these matters are of importance to their work.
- Personal data made available to Vasion in the course of the Services is used solely for the agreed-upon purpose. Therefore, Vasion only processes personal data temporarily and for its intended purpose. At the end of the Agreement, after the completion of providing the agreed-upon Services or upon the request of the Customer, Vasion promptly returns or irretrievably deletes all Customer Data. In this regard, any supplemental agreements shall be taken into account.

3. Data Security and Preservation Controls:

Vasion takes the following measures to protect Customer Data.

- For encryption and protection of data during transmission and storage, all data is transported over https using TLS 1.2 and at rest with AWS 256.

- Customer Data is backed up daily/weekly. Daily backups are kept for seven days, weekly backups are kept for six months. Backup objects are encrypted using server-side encryption with either Amazon S3-managed keys (SSE-3) or AWS KMS-managed keys (SSE-KMS).
- For data recovery and business resiliency, Vasion utilizes multiple availability zones within AWS. In the extreme event that all availability zones become unavailable, Vasion can utilize CloudFormation templates to rebuild infrastructure in a different region.
- Vasion separates Customer Data to prevent malicious or compromised users from affecting the service or data of another service.
- Vasion governs security to coordinate and direct its overall approach to the management of the service and information within industry standard security policies and security standards, defined responsibilities and risk based decision-making authority processes.
- Operational Security- Vasion has processes and procedures in place to ensure the operational security of the service provided including configuration and change management, security patch management, vulnerability management, protective monitoring, security incident management and secure decommissioning.
- Secure Development – Vasion ensures that all software it develops and provides as part of its Services has been developed following a secure software development lifecycle process which includes industry best practices for achieving and sustaining required security qualities for confidentiality, integrity and availability protection.
- Vasion ensures that the methods used by administrators to manage the operational service are designed to mitigate any risk of exploitation that could undermine the security of the Services. Remote administration sessions must be encrypted, use at least two-factor for authentication, access to the systems administered must be restricted by IP addresses used by Vasion by means of access control lists.
- Vasion ensures to monitor and document the reliability, maintainability, serviceability and availability of a system or service on a continuous basis. For the Vasion solution, Vasion provides a Service Level Agreement identifying a minimum availability of 99.5% per month.

ANNEX C

LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

VASION AUTOMATE PLATFORM:

Name	Address	Contact person's name, position, and contact details	Description of processing
Amazon Web Services	www.amazon.com	N/A	Cloud hosting
Microsoft Azure	azure.microsoft.com	N/A	Cloud hosting
Datadog	Datadog.com	N/A	SaaS platform that integrates and automates infrastructure monitoring, application performance monitoring and log management.

*For the Vasion Print to Scan functionality, the following sub-processor is used in addition to Amazon Web Services or Microsoft Azure:

Name	Address	Contact person's name, position, and contact details	Description of processing
AWS SES	aws.amazon.com/workmail	N/A	Use of email SMTP relay and flexible HTTP API for routing scans to email.