Data Processing Agreement

This Data Processing Addendum, along with its appendices ("**DPA**"), is an integral part of the Agreement and applies whenever Patchworks and/or its Affiliates ("**Patchworks**") provides to the Customer the Patchworks' products and/or services as detailed in the Agreement ("**Services**") that involve the processing of Customer's Personal Data (as defined below) subject to Applicable Data Protection Laws.

1. DEFINITIONS

Capitalised terms not otherwise defined below or otherwise in this DPA shall have the meaning given to them in the Agreement:

1.1 **Agreement** means, for the purposes of this DPA, the main agreement entered into between Patchworks and the Customer containing the terms and conditions relating to the provision and use of the Patchwork's Services as detailed in such agreement.

1.2 **Applicable Data Protection Laws** means as applicable and as updated, (i) applicable Swiss privacy laws, (ii) GDPR, (iii) UK GDPR, (iv) UK Data Protection Act 2018, and (iv) CPRA, and (v) any other privacy laws that regulate the Processing of Personal Data by Patchworks in connection with the provision of its products and/or service as detailed in the Agreement that the parties agree in writing are applicable from time to time.

1.3 **Controller** means an entity that determines the purpose and means of Processing of the Personal Data.

1.4 **CPRA** means the California Consumer Privacy Act of 2018 (CCPA) as further amended and modified by the California Privacy Rights Act, Cal. Civ. Code § 1798.100 *et seq*.

1.5 **Customer Data** means the Customer's data provided to Patchworks or otherwise uploaded, entered or submitted by or on behalf of the Customer into or via the Patchworks' Services as detailed in the Agreement.

1.6 **Data Subject** means the individual to whom the Personal Data relates.

1.7 **Documented Instructions** has the meaning given in clause 3.7(a).

1.8 **EU SCCs** means the agreement, incorporated by reference under clause 4.2(a) of this DPA by and between Customer and Patchworks, pursuant to the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

1.9 **GDPR**: means 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, and repealing Directive 95/46/EC.

1.10 **Personal Data** means "personal data" or "personal information" (or any analogous concept) under the applicable privacy law, including Applicable Data Protection Laws, that forms part of the Customer Data and is Processed by Patchworks as Processor (or its Sub-processors) as part of provision of Patchworks's

Services as detailed in the Agreement.

1.11 **Processing** means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.12 **Processor** means an entity that Processes Personal Data directly or indirectly on behalf of a Controller.

1.13 **Services** has the meaning given in the first paragraph above.

1.14 **Sub-processor** means any Processor engaged by Patchworks and involved in the Processing of Personal Data.

1.15 **UK GDPR** means GDPR as it applies under UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018.

1.16 **UK SCCs** means the International Data Transfer Addendum to the EU SCCs, issued by the Information Commissioner's Office under s.119A (1) of the United Kingdom Data Protection Act 2018 and incorporated by reference under clause 4.2(b) of this DPA by and between Customer and Patchworks.

2. INTERPRETATION

2.1 Patchworks provides the Services purchased by the Customer as defined in the Agreement, and it will Process Personal Data in connection with such Services. Such Processing is governed by the terms and conditions of this DPA, which is hereby incorporated by reference into the Agreement.

2.2 In the event of any inconsistency among the following documents, the order of precedence will be: (i) the terms of this DPA; and (ii) the Agreement.

3. DATA PROTECTION OBLIGATIONS

3.1 Each party will comply with the requirements of Applicable Data Protection Laws which are applicable to that party.

3.2 In relation to the Personal Data, Appendix 1 sets out the scope, nature and purpose of Processing by Patchworks, the duration of the Processing, the types of Personal Data and the categories of Data Subjects.

3.3 The parties have determined that, for the purposes of Applicable Data Protection Laws, Patchworks shall Process the Personal Data as a Processor on behalf of the Customer in respect of the Processing activities set out in Appendix 1. Should the determination in this 3.2 change, then each party shall work together in good faith to make any changes which are necessary to this DPA or the related appendices, as applicable.

3.4 The Customer acknowledges and agrees that (i) Patchworks is not able or required to verify the residency of each Data Subject, (ii) the Customer solely determines whether to submit any Personal Data for

Processing by the Patchworks's Services detailed in the Agreement, and (iii) the Customer is solely responsible for, and shall ensure that:

a) the Documented Instructions comply at all times with all applicable privacy laws, including Applicable Data Protection Laws, and that all Personal Data may be Processed by Patchworks in compliance with such laws. In the event either party is or becomes aware that those instructions are in conflict with any applicable privacy law, including any Applicable Data Protection Law, each party will promptly notify the other party in writing and the parties will work together to resolve any such conflict, provided that Patchworks shall be entitled to:

(i) charge the Customer for any agreed changes reasonably required to its products and services, related procedures and/or this DPA; or

(ii) terminate the relevant Agreement and/or related Order Form (1) where the required changes impose an excessive burden on Patchworks, make the Services substantially different to the existing ones or are not technically feasible, or (2) after the Customer has become aware that its instructions infringe applicable legal requirements, the Customer insists on compliance with those instructions.

3.5 Without prejudice to the generality of clause 3.1, the Customer shall ensure that it has all necessary and appropriate rights, consents and notices in place to enable the lawful transfer of Personal Data to and processing of Personal Data by Patchworks for the duration and purposes of this DPA and in accordance with the Documented Instructions.

3.6 Without prejudice to the generality of clause 3.1, in relation to the Personal Data, Patchworks shall:

(a) Process that Personal Data only on the Documented Instructions defined herein. This DPA, the Agreement (including any related Order Forms), Customer's instructions via its use of the Services and related APIs and Tools made available by Patchworks as part of the Services in accordance with the Agreement and the nature and purposes of processing (along with the subject-matter, types of Personal Data and data subjects and duration of processing) set out in Appendix 1 constitute the complete set of instructions to Patchworks in relation to the Processing of Personal Data ("**Documented Instructions**"), unless Patchworks is required by applicable laws to otherwise Process that Personal Data. Where Patchworks is relying on applicable laws as the basis for Processing Customer Processor Data, Patchworks shall notify the Customer of this before performing the Processing required by the applicable laws unless those applicable laws prohibit the Provider from so notifying the Customer on important grounds of public interest;

(b) in accordance with applicable Data Protection Laws, implement appropriate technical and organisational measures to protect against unauthorised or unlawful Processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data, which are appropriate to the harm that might result from the unauthorised or unlawful Processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures;

(c) ensure that any personnel engaged and authorised by Patchworks to Process Personal Data have committed themselves to confidentiality or are under an appropriate statutory or common law obligation of confidentiality;

(d) assist the Customer insofar as this is possible (taking into account the nature of the Processing and the information available to Patchworks), and at the Customer's cost and written request, in

responding to any request from a Data Subject and in ensuring the Customer's compliance with its obligations under Applicable Data Protection Laws with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators;

(e) notify the Customer without undue delay on becoming aware of any actual unauthorised disclosure of, or accidental or unlawful destruction, loss, compromise, damage or theft of Personal Data or any incidents or set of events, including any that give rise to a 'personal data breach" (as such term, or any analogous terms, is defined under Applicable Data Protection Law) involving the Personal Data;

(f) at the written direction of the Customer, delete or return Personal Data and copies thereof to the Customer within 30 days of the date of termination of the Agreement unless limited retention by Patchworks is required such as for back up purposes or where Patchworks is otherwise required by Applicable Data Protection Law or other applicable law to continue to Process that Personal Data. For the purposes of this clause 3.6(f), Personal Data shall be considered deleted where it is put beyond further use by Patchworks; and

(g) maintain records to demonstrate its compliance with the terms of this DPA, and allow for reasonable related audits conducted by the Customer, the Customer's designated auditor for this purpose, or a competent supervisory authority under Applicable Data Protection Laws; provided that the Customer shall pay Patchworks's reasonable costs and expenses incurred in connection with such audit and such audit (i) is following reasonable prior written notice (at least 30 days) to Patchworks; (ii) is no more than once per year (except where mandated by a competent regulatory authority), (iii) is subject to reasonable confidentiality and security controls, and (iv) does not unreasonably interfere with Patchworks's day to day business activities. The Customer shall comply with Patchworks's reasonable security requirements.

3.7 The Customer hereby provides its prior, general authorisation for Patchworks to appoint Sub-Processors to Process the Personal Data. Patchworks's then current Sub-processors as at the Effective Date of the Agreement are set out in Appendix 2. Patchworks shall:

(h) ensure that the terms on which it appoints such Sub-processors comply with Applicable Data Protection Laws, and are similar in substance to those terms set out in this DPA;

(i) where, and to the extent, required under Applicable Data Protection Laws, be liable for the performance of its Sub-processors to the same extent Patchworks would be liable if Processing Personal Data itself; and

(j) inform the Customer of any intended changes concerning the addition or replacement of the Sub-processors at least 30 days in advance, thereby giving the Customer the opportunity to object to such changes provided that such objection is based on reasonable grounds relating to data protection. If no objection has been received by Patchworks within 30 days of the date of notice of such change, the Customer shall be deemed to have accepted such change. The parties agree to act reasonably and in good faith to resolve any objection by the Customer received within the objection period.

To the extent any audit undertaken by the Customer pursuant to clause 3.6(g) requires information relating to a Sub-processor, the Customer acknowledges that such information may only be obtained in accordance with the terms of the relevant Sub-processor agreement.

4. CROSS-BORDER TRANSFERS

4.1 The Customer hereby gives Patchworks its prior, general authorisation for Patchworks to transfer Personal Data outside of the EEA, Switzerland and/or UK as required for the purposes specified in Appendix 1, provided that Patchworks shall ensure that all such transfers are effected in accordance with Applicable Data Protection Laws.

4.2 Where the Personal Data is being transferred by the Customer from the European Economic Area ("*EEA*"), the United Kingdom or Switzerland for Processing by Patchworks in a country outside of those jurisdictions, the parties agree that where an adequacy decision or other transfer mechanism in accordance with Applicable Data Protection Laws is not in place:

(a) the EU SCCs will apply to Personal Data that is transferred from the EEA or Switzerland, either directly or via onward transfer, to any country or recipient outside of the EEA or Switzerland that is not recognised by the competent EEA or Swiss regulatory authority or governmental body for the EEA or Switzerland (as applicable) as providing an adequate level of protection for personal data. For data transfers from the EEA or Switzerland that are subject to the EU SCCs, the EU SCCs will be deemed entered into and incorporated into this DPA by this reference and completed as set out in Appendix 3; and

(b) the UK SCCs will apply to Personal Data that is transferred from the United Kingdom, either directly or via onward transfer, to any country or recipient outside of the United Kingdom that is not recognised by the competent United Kingdom regulatory authority or governmental body for the United Kingdom as providing an adequate level of protection for personal data. For data transfers from the United Kingdom that are subject to the UK SCCs, the UK SCCs will be deemed entered into and incorporated into this DPA by this reference and completed as set out in Appendix 4.

4.3 Where the Applicable Data Protection Law of a jurisdiction other than the EEA, the United Kingdom or Switzerland applies to the Personal Data and requires the parties to enter into a set of standard contractual clauses to protect the transfer of Personal Data outside of that jurisdiction and no alternative mechanism, such as an adequacy decision, is available or applicable, the parties shall negotiate a related amendment to this DPA acting reasonably and in good faith.

4.4 By entering into the Agreement, where applicable, the parties are deemed to have signed the relevant SCCs incorporated herein, including their Annexes, as of the effective date of the Agreement or as at the date they become applicable (based on a corresponding change in Documented Instructions).

5. CPRA. Where the CPRA applies to any Personal Data Processed by Patchworks under this DPA, in addition to the above terms and conditions, the parties agree that: (a) the Customer only discloses the Personal Data to enable Patchworks to process Personal Data pursuant to this DPA; and (b) Patchworks (i) will not 'sell' or 'share' (as those terms are defined in the CPRA) Personal Data (or be required by the Customer to do so); (ii) will not retain, use, or disclose Personal Data for any purpose, including any commercial purpose, except as permitted in the Agreement, the DPA or under CPRA; (iii) will not retain, use, or disclose Personal Data outside the direct business relationship between Patchworks and the Customer, including by not combining any Personal Data with other Personal Data collected or received from another source, except as permitted by CPRA; (iv) Patchworks will notify the Customer in accordance with clause 6.1 of this DPA if it determines that it can no longer meet its obligations under CPRA; and (v) if Patchworks

is engaged in unauthorised use of Personal Data, Customer may, upon reasonable notice to Patchworks, take reasonable and appropriate steps to stop and remediate such unauthorised use of the Personal Data.

6. LIABILITY

This DPA is subject to the indemnification and limitations of liability provisions of the Agreement.

7. MISCELLANEOUS

7.1 Notifications. Notices required to be given by Patchworks under this DPA or the Agreement to notify the Customer of any changes to the Processing of Personal Data under this DPA, Patchworks will notify the Customer by sending an email to the Customer's nominated representative.

7.2 Amendments to this DPA: Patchworks may amend this DPA from time to time by posting a revised version on its website or by otherwise notifying the Customer in accordance with clause 7.1 of this DPA. Patchworks will notify Customer of any material changes to this DPA and any amended terms will become effective upon posting or, if Patchworks notifies the Customer by email, on the date specified in such email. By continuing to use the Services after the effective date of any such amended terms, the Customer agrees to be bound by such amended terms. It is Customers responsibility to check Patchwork's website regularly for changes to this DPA.

7.3 Governing law. This DPA shall be governed and construed in accordance with the laws governing the Agreement.

Appendix 1 – Processing, Personal Data and Data Subjects

1. Processing by the Provider – Scope/Subject Matter, Nature and Purpose

Patchworks Integration Platform as a Service (iPaaS) handles personal data when transmitting and/or transforming customer and order data between eCommerce, Enterprise Resource Planning (ERP), Customer Relationship Management (CRM), Email Service Providers (ESP) and other systems and platforms.

All data is transmitted and received via secure communication methods and, where appropriate, data is encrypted.

Where Patchworks iPaaS transmits and/or transforms customer/contact data independently (i.e., not as part of an order update or other associated service), email addresses are stored for logging and matching purposes. In addition, when Patchworks iPaaS transmits and/or transforms Personal Data, the payload data (including customer and order details) and associated run logs are stored temporarily, for no longer than 7 days, so that failed transfers can be investigated and resolved. They are then deleted automatically.

2. Duration of the Processing

Personal Data is retained from the point of initial transmission/transformation for the duration of the Agreement and for a period of 30 days from the date of termination of the Agreement to allow for the return or deletion of such data, except for any Personal Data which may be retained under applicable Data Protection Law or any other applicable laws. Any retained Personal Data will continue to be protected in accordance with this DPA. Personal Data can be deleted more frequently upon request. Within that period, the following maximum retention

periods apply: (i) payload data and run logs are deleted automatically 7 days after processing; (ii) email addresses stored for logging and matching are retained for the duration of the Agreement; and (iii) backups expire automatically after 7 days. Where the Services are provided through the Patchworks Shopify app, all data relating to a shop is deleted within 72 hours of Patchworks receiving Shopify's shop/redact notification following uninstallation of the app, and the relevant customer's data is deleted on receipt of a customers/redact request. For any access, update or deletion requests with regard to your customers' personal data, please email security@patchworks.io

Limited retention of Personal Data may occur in some cases, such as backups; however, if this occurs, these are secured and placed beyond use. Backups are encrypted, access-restricted and expire automatically after 7 days. For a copy of Patchworks' Retention Schedule (document 0030), or for any further questions with regard to the portability, security and auditing of data, please contact us at security@patchworks.io.

3. Types of Personal Data

The types of personal data that the Customer may submit are determined and controlled solely at the Customer's discretion and may include, but are not limited to, the following categories: name, address, email address, telephone number, fax number, order and transaction details (such as order numbers, products purchased, order values, and delivery and billing addresses), other contact details and associated local time zone data.

3. Categories of Data Subject

- Customers
- Interested parties
- Partners
- Suppliers
- Employees
- Contractors

4. Special Categories of Data

No sensitive or health-related or special category of personal data is required for the provision of Patchworks's Services, and submitting such data for Processing is prohibited except in circumstances where the Customer has obtained the prior written agreement of an authorised representative of Patchworks (which agreement may be subject to additional requirements and terms).

APPENDIX 2 – SUB-PROCESSORS

Name of Sub-processor	Company details	Nature of processing	Duration of processing	Place of performance of core Processing activities
AWS	CSP	Hosting & Analytics	For as long as required under the Agreement	EU West (London)
CloudFlare	Network Services	Secure Network Transport	For as long as required under the Agreement	GB
Atlassian	Project & Workflow	Project Management	For as long as required under the Agreement	UK, EU, US
Vercel	Infrastructure	Web Framework	For as long as required under the Agreement	US, EU, UK
Sentry	Monitoring	Monitoring	For as long as required under the Agreement	US
Elastic	Search	Search	For as long as required under the Agreement	EU West (London)
MailGun	Email	Email	For as long as required under the Agreement	EU
DevTeam	Support	Support Services	For as long as required under the Agreement	Philippines
Hashicorp Vault	Security	Vault	For as long as required under the Agreement	UK
Hasura	GraphQL	API	For as long as required under the Agreement	UK

APPENDIX 3 – EU SCCS

PART A – EU SCCs Schedule to the DPA

This EU SCCs Schedule applies if the EU SCCs apply as set forth in clause 4.2(a) of the DPA.

1. Processing Generally.

a. *Modules.* Customer and Patchworks acknowledge and agree that Module 2 (Transfer Controller to Processor) of the EU SCCs applies to the Processing of Personal Data described in the DPA.

b. *Instructions.* Customer's complete and final documented instructions for the Processing of Personal Data for the purposes of the EU SCCs, including clause 8.1(a) of the EU SCCs, are those referred to in clause 3.6 of the DPA.

c. *Deletion.* The parties acknowledge and agree that any deletion or return of Personal Data that is described in clause 8.5 of the EU SCCs (and certification of the same) shall be conducted as set forth in clause 3.6 of the DPA, and a certification shall be provided by Patchworks only upon Customer's request.

d. *Onward Transfers.* The parties acknowledge and agree that Customer's documented instructions for disclosure of Personal Data to a third party as described in clause 8.8 of the EU SCCs shall be carried out in accordance with clauses 3.7 and 4 of the DPA.

e. *Access by public authorities.* Customer agrees to reimburse Patchworks for all reasonable fees, costs and expenses (including reasonable legal fees) it incurs in complying with its obligations under clause 15 of the of the EU SCCs.

2. Sub-processors.

The parties agree to use Option 2 in clause 9(a) of the EU SCCs, and that changes to Sub-processors as described under clause 9(a) shall be dealt with in accordance with clause 3.7 of the DPA. The parties agree that the copies of the Sub-processor agreements that must be provided by Patchworks to Customer pursuant to clause 9(c) of the EU SCCs may have all commercial information, or clauses unrelated to the EU SCCs or their equivalent, removed by Patchworks beforehand; and, that such copies will be provided by Patchworks, in a manner to be determined in its discretion, only upon written request by Customer.

3. Governing Law.

The parties agree to use Option 1 set forth in clause 17 of the EU SCCs. The Parties agree that the law of Ireland. Furthermore, the parties agree to use the courts of Ireland for purposes of clause 18 of the EU SCCs.

4. Miscellaneous.

The parties agree that: (i) in clause 7 of the EU SCCs, the optional docking clause will apply; (ii) in clause 11 of the EU SCCs, the optional language will not apply; (iii) in respect of Switzerland, the EU SCCs will apply provided that any references in the clauses to the GDPR shall refer to the FADP; the FDPIC is the competent supervisory authority; the term 'member state' must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence in accordance with

clause 18(c) of the clauses and the clauses shall also protect the data of legal persons until the entry into force of the revised FADP).

5. Annexes to EU SCCs

a. *Annex I of EU SCCs.* Annex I of the EU SCCs is completed as set out in Annex 1 of this Appendix 3.

b. *Annex II of EU SCCs.* Annex II of the EU SCCs is completed as set out in Annex 2 of this Appendix 3.

Annex 1 of Appendix 3

A. LIST OF PARTIES

Data exporter(s): Customer (as defined in the Agreement)

Contact person's name, position and contact details: the contact details specified by the Customer in the Agreement
Activities relevant to the data transferred under these Clauses: see part B. below
Role (controller/processor): controller

Data importer(s): Patchworks (as defined in the DPA)

Contact details: security@patchworks.io
Activities relevant to the data transferred under these Clauses: see Part B. below
Role (controller/processor): processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred
As per the Documented Instructions including Appendix 1 of the DPA.

Categories of personal data transferred
As per the Documented Instructions including Appendix 1 of the DPA.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

As per the Documented Instructions including Appendix 1 of the DPA.

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

Nature of the processing
The nature of the Processing is the provision and performance of the Patchworks's Services pursuant to the Agreement.

Purpose(s) of the data transfer and further processing
The purpose of the Processing is the provision and performance of the Patchworks's Services pursuant to the Agreement.

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

Personal Data will be retained by the data importer no longer than necessary for the purposes set forth in the Agreement and in accordance with the DPA.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

The subject matter, nature and duration of the processing are the provision and performance of the Patchworks's Services pursuant to the Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer shall act as competent supervisory authority.

Annex 2 of Appendix 3

Technical & Organisational Security Measures

These practices are subject to ongoing technical progress and development. Patchworks may update or modify them, provided that such changes do not diminish the overall security of the Services Patchworks provides under the Agreement.

1. **Measures of encryption of personal data and pseudonymisation**
   TLS 1.2 or above is used as Full (Strict) encryption via Cloudflare Edge Certificates using verified CA. AES 265 is used for data at rest using AWS infrastructure encryption. Data masking on PII data.

2. **Measures to ensure the continuous confidentiality, integrity, availability, and resilience of processing systems and services include:**
   Continuous Monitoring is in place with alerting. Environments are split between production, stage, and development to ensure availability. Encryption, SSO and the principle of least privilege are implemented to ensure confidentiality. Hashing algorithms and data sanitisation are needed for data integrity, and a rigorous testing process is needed to ensure the platform's code quality and functionality/ resilience.

3. **Measures to ensure the timely restoration of availability and access to personal data in the event of a physical or technical incident include:**
   We have a detailed BC/DR plan to restore our critical services in the event of outages. This includes an Incident Response Policy. Backups are kept to ensure redundancy across environments.

4. **Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures to ensure data processing security.**
   Established ISMS and policy suite to ensure processes exist to ensure data processing security. Maintaining ISO27001 and achieving SOC2 attestation has ensured process is followed across the organisation.

5. **Measures for authorisation and identification of a user**
   SSO is implemented on our main Google X AWS account. MFA is implemented on our critical and main systems. Principle of least privilege is followed.

6. **Measures to protect data during transmission**

   TLS 1.2 and above is used for network transmission along with favouring SFTP for file transfers. S3 File storage is protected with access control.

7. **Measures for the protection of data during storage**

   Encryption at rest as detailed in 1.

8. **Measures to ensure the physical security of locations where personal data is processed**

   AWS Infrastructure data centre protections.

9. **Measures for ensuring events logging**

   Grafana, Loki, AWS CloudWatch, AWS CloudTrail and Wazuh used for event logging.

10. **Measures to ensure proper system configuration, including default settings**

    Strict access control to main Dev, DevOps and Security tools using the principle of least privilege. change and audit logs to track changes and documentation to ensure knowledge transfer.

11. **Measures for ensuring limited data retention**

    GDPR Statement and deletion request information publicly available. Data retention in line with our data retention schedule. Policy and processes established to ensure limited timings and schedules on data retention, storage and processing. Lifecycle policy on storage including AWS S3. Integration payloads are deleted automatically after 7 days by AWS S3 lifecycle expiration rules, and run logs are deleted after 7 days by a daily scheduled purge job logged in Loki. Backups expire automatically after 7 days. Shopify's mandatory privacy webhooks (customers/data_request, customers/redact and shop/redact) are processed and each event is logged. Engineering and the Document Owner review deletion logs and offboarding tickets quarterly to confirm deletion is working.

12. **Measures for allowing data portability and ensuring erasure**

    Data backups are kept in AWS along with snapshots, volumes and other storage allowing data portability where required. Machine images are kept and managed. All follow a lifecycle policy setup and maintained in AWS.

APPENDIX 4 – UK SCCs

UK SCCs

This UK SCCs Schedule applies if the UK SCCs apply as set forth in clause 4.2(b) of the DPA. **Appendix 3** of this DPA is hereby incorporated by reference into this Appendix 4 and applies to the UK SCCs in the same way and to the same extent as it does for the EU SCCs (except to the extent expressly amended by the UK SCCs).

Part 1: Tables of the UK SCCs are completed as set forth below:

Table 1: Parties

The parties' details and key contact information is as set out in Annex 1A of Appendix 3 of this DPA.

Table 2: Selected SCCs, Modules and Selected Clauses

The Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

- Module 2 only
- Clause 7 (Docking clause): this optional clause will apply
- Clause 11: this optional clause will not apply
- Clause 9a (Prior Authorisation or General Authorisation): Option 2 (general authorisation) will apply.
- Clause 9a (Time Period): the time period set out in clause 3.7 of the DPA

Table 3: Appendix Information

Annex IA: the list of Parties is set out in Annex 1A of Appendix 3 of this DPA.
Annex IB: the description of the transfer is set out in Annex 1A of Appendix 3 of this DPA.
Annex II: the technical and organisational measures (including technical and organisational measures to ensure the security of the data) are set out in Annex 2 of Appendix 3 of this DPA.
Annex III: the list of Sub-processors is set out in Appendix 2 of this DPA.

Table 4: Ending this Addendum when the Approved Addendum Changes

Both the Exporter and the Importer may end this Addendum as set out in section 19 of the UK SCCs.