Uniform Systems, Inc. Data Processing Agreement

Updated June 21, 2024

This Data Protection Agreement (the "DPA") is incorporated into and made part of the Master Subscription Agreement (the "Agreement") between Uniform Systems, Inc. ("Uniform") and the customer identified in the Agreement ("Customer") and pertains to Uniform's protection of Customer-provided personal data when Customer uses the Service. Capitalized terms have the meanings provided in the Agreement except as provided here.

1. **Definitions**. In this DPA, the following terms shall have the following meanings:

1.1. "controller", "processor", "data subject", "personal data", "processing" (and "process") and "special categories of personal data" shall have the meanings given in Applicable Data Protection Law; and

1.2. "Applicable Data Protection Law" shall mean the GDPR, the UK Data Protection Laws, US Data Protection Laws and all other data protection and privacy laws and regulations of the United States, the United Kingdom and the EEA applicable to the processing of personal data under the Agreement.

1.3. "EEA" means the European Economic Area, which constitutes the member states of the European Union and Iceland, Liechtenstein, Norway and Switzerland.

1.4. "GDPR" means the General Data Protection Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

1.5. "Standard Contractual Clauses" means the Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries under GDPR, as approved by European Commission Implementing Decision 2021/914. Appendix 1 to this DPA contains certain interpretive and supplementary provisions regarding application of the Standard Contractual Clauses. The information required by Annexes 1 and 2 of the Standard Contractual Clauses is provided in Annexes 1 and 2 of this DPA.

1.6. "UK Data Protection Laws" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act of 2018 and the Data Protection Act 2018.

1.7. "US Data Protection Laws" means the California Consumer Privacy Act as amended by the California Privacy Rights Act and its associated regulations and their successors and all other US state and federal laws, regulations and rules applicable to the protection of personal data, which as of the date of publication of this DPA include the Colorado Privacy Act, Connecticut Personal Data Privacy and Online Monitoring Act, Indiana Consumer Data Protection Act, Iowa Consumer Data Protection Act, Montana Consumer Data Privacy Act, Tennessee Information Protection Act, Texas Data Privacy and Security Act, Utah Consumer Privacy Act and Virginia Consumer Data Protection Act.

2. Data Protection.

2.1. Relationship of the Parties. Customer (the controller) appoints Uniform as a processor to process the personal data described in the Agreement (the "Data") only for the

limited and specific purpose of providing the data integrity management Service(s) identified in each Order Form executed by the parties or as otherwise agreed in writing by the parties (the "Permitted Purpose"). Each party shall comply with the obligations that apply to it under Applicable Data Protection Law. Uniform shall promptly inform Customer if it: (a) becomes aware that processing for the Permitted Purpose infringes Applicable Data Protection Law, or (b) determines it can no longer meet its obligations under this DPA or Applicable Data Protection Law.

2.2. Processing in Accordance with US Data Protection Law. With respect to personal data to which US Data Protection Law applies Uniform will not: (a) “sell” (as defined in applicable laws) any personal data; (b) collect, share, retain, use or disclose any personal data except as necessary to perform services for Customer; or (c) use personal data outside the direct business relationship between the parties. Customer has the right, upon notice to Uniform, to take reasonable and appropriate steps to ensure that Uniform uses personal data in a manner that is consistent with Customer’s obligations under Applicable Data Protection Law and to stop and remediate unauthorized use of personal data.

2.3. International transfers. Uniform shall not transfer the Data outside of the EEA unless it has taken such measures as are necessary to ensure the transfer is in compliance with Applicable Data Protection Law.

2.4. Confidentiality of processing: Uniform shall ensure that any person it authorises to process the Data (an "Authorised Person") shall protect the Data in accordance with Uniform's confidentiality obligations under the Agreement.

2.5. Security: Uniform shall implement technical and organisational measures as set out in the **Annex** to protect the Data (a) from accidental or unlawful destruction, and (b) loss, alteration, unauthorised disclosure of, or access to the Data (a "Security Incident").

2.6. Subprocessors: Customer consents to Uniform engaging the third party subprocessors listed in Exhibit A to process the Data for the Permitted Purpose provided that it: (a) will inform Customer of any intended changes concerning the addition or replacement of other subprocessors, thereby giving Customer the opportunity to object to such changes; (b) imposes data protection terms on any subprocessor it appoints that require it to protect the Data to the standard required by Applicable Data Protection Law; and (c) remains liable for any breach of this Clause that is caused by an act, error or omission of its subprocessor. Customer may object to Uniform’s appointment or replacement of a subprocessor prior to its appointment or replacement, provided such objection is based on reasonable grounds relating to data protection. In such event, Uniform will either not appoint or replace the subprocessor or, if this is not possible, Customer may suspend or terminate the Agreement (without prejudice to any fees incurred by Customer prior to suspension or termination).

2.7. Cooperation and Data Subjects' Rights. Uniform shall provide reasonable and timely assistance to Customer (at Customer’s expense) to enable Customer to respond to: (a) 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 (b) any other correspondence, enquiry or complaint received from a data subject, regulator or other third party in connection with the processing of the Data. In the event that any such request, correspondence, enquiry or complaint is made directly to Uniform, Uniform shall promptly inform Customer providing full details of the same.

2.8. Data Protection Impact Assessment. Uniform shall provide reasonable cooperation to Customer (at Customer's expense) in connection with any data protection impact assessment that Customer may be required under Applicable Data Protection Law.

2.9. Security Incidents. If it becomes aware of a confirmed Security Incident, Uniform shall inform Customer without undue delay and shall provide reasonable information and cooperation to Customer so that Customer can fulfil any data breach reporting obligations it may have under (and in accordance with the timescales required by) Applicable Data Protection Law. Uniform shall further take such any reasonably necessary measures and actions to remedy or mitigate the effects of the Security Incident and shall keep Customer informed of all material developments in connection with the Security Incident.

2.10. Deletion or Return of Data. Upon termination or expiry of the Agreement, Uniform shall (at Customer's election) destroy or return to Customer all Data in its possession or control. This requirement shall not apply to the extent that Uniform is required by applicable law to retain some or all of the Data, or to Data it has archived on back-up systems, in which event Uniform shall securely isolate and protect from any further processing except to the extent required by such law.

2.11. Audit. Customer acknowledges that Uniform is audited against SOC 2 standards by independent third party auditors. Upon request and when available, Uniform shall supply a summary copy of its audit report(s) to Customer, which shall be subject to the confidentiality provisions of the Agreement. Uniform shall also respond to any written audit questions submitted to it by Customer, provided that Customer shall not exercise this right more than once per year. In addition, Customer may contact Uniform to request an on-site audit, not more than once per year, of the procedures relevant to the protection of Customer's personal data. Before the commencement of any such on-site audit, Customer and Uniform shall mutually agree upon the scope, timing, and duration of the audit and the reimbursement rate for any travel or other expenses Uniform incurs in the course of such audit. All reimbursement rates shall be reasonable, taking into account the resources expended by Uniform. Customer shall promptly notify Uniform with information regarding any non-compliance discovered during the course of an audit.

3. Miscellaneous.

3.1. Construction; Interpretation. This DPA is not a standalone agreement and is only effective if the Agreement is in effect between Customer and Uniform. This DPA is part of the Agreement and is governed by its terms and conditions, including the limitations of liability therein. This DPA and the Agreement are the complete and exclusive statement of the mutual understanding of the parties and supersede and cancel all previous written and oral agreements and communications relating to the subject matter hereof. Headings contained in this DPA are for convenience of reference only and do not form part of this DPA.

3.2. Severability. If any provision of this DPA is adjudicated invalid or unenforceable, this DPA will be amended to the minimum extent necessary to achieve, to the maximum extent possible, the same legal and commercial effect originally intended by the parties. To the extent permitted by applicable law, the parties waive any provision of law that would render any clause of this DPA prohibited or unenforceable in any respect.

3.3. Amendment; Enforcement of Rights. No modification of or amendment to this DPA, nor any waiver of any rights under this DPA, will be effective unless in writing signed by the parties to this DPA. The failure by either party to enforce any rights under this DPA will not be construed as a waiver of any rights of such party.

3.4. Assignment. This DPA may be assigned only in connection with a valid assignment pursuant to the Agreement. If the Agreement is assigned by a party in accordance with its terms, this DPA will be automatically assigned by the same party to the same assignee.

3.5. Governing Law. This DPA will be governed by and construed in accordance with the laws the jurisdiction governing the Agreement unless otherwise required by Applicable Data Protection Law, in which case this DPA will be governed by the laws of the Republic of Ireland.

Exhibit A – Subprocessor(s)

Company: Hasura

Data processing activity: GraphQL Server

Location: United States, Germany

Contact information: 355 Bryant Street, Unit 403, San Francisco, CA 94107

Company: Auth0

Data processing activity: Cloud Identity and Authorization Services

Location: United States

Contact information: 10800 NE 8th St, Suite 700 Bellevue, WA 98004

Company: Sentry

Data processing activity: Error Reporting

Location: United States

Contact information: 45 Fremont Street, 8th Floor, San Francisco, CA 94105

Company: Hubspot

Data processing activity: Cloud Marketing and Client Relationship management

Location: United States

Contact information: 25 1st St, 2nd Fl Cambridge, MA 02141

Company: Pendo.io

Data processing activity: Usage analytics

Location: United States

Contact information: 150 Fayetteville St. Raleigh, NC 27601 USA

Appendix 1 – Applicable Standard Contractual Clauses and Supplemental Terms

1. Incorporation of Standard Contractual Clauses

The parties agree that the Standard Contractual Clauses are hereby incorporated by reference into this DPA as follows:

1.1 Where Uniform processes personal data as a processor pursuant to the terms of the Agreement, Uniform and its relevant subprocessor affiliates are located in non-adequacy approved third countries, and Customer and its relevant affiliates are established in the EEA, **Module 2: Transfer controller to processor**, Clauses 1 to 6 and 8 to 18 apply.

1.2 Where Uniform processes personal data as a processor pursuant to the terms of the Agreement, Uniform and its relevant subprocessor affiliates are located in non-adequacy approved third countries, and Customer and its relevant Affiliates are established in the EEA, **Module 3: Transfer processor to processor**, Clauses 1 to 6 and 8 to 18 apply.

2. Standard Contractual Clause Option Provisions

Where the Standard Contractual Clauses identify optional provisions (or provisions with multiple options) the following shall apply in the following manner:

2.1 Clause 7 (Docking Clause) is omitted;

2.2 In Clause 9(a) (Use of sub-processors) – Option 2 shall apply and the parties shall follow the process and timings agreed in the DPA to appoint sub-processors;

2.3 In Clause 11(a) (Redress) – the Optional provision shall NOT apply; and

2.4 In Clause 16(b) (Suspension of transfers) if Uniform is the data exporter it will suspend transfers of personal data only as required by law and will notify Customer as promptly as possible (before suspension if possible) so that Customer may remedy the condition requiring suspension.

3. EU Optional Provisions

3.1 In Clause 17 (Governing Law)– the laws of the Republic of Ireland shall govern; and

3.2 In Clause 18 (Choice of forum and jurisdiction) – the courts of the Republic of Ireland shall have jurisdiction.

4. Swiss Law Provisions

4.1 With respect to Personal Data transferred from Switzerland for which Swiss law governs:

(a) references to the EU, member states and GDPR in the Standard Contractual Clauses are amended mutatis mutandis to refer to Switzerland, the Swiss Federal Data Protection

Act (as it may be updated or replaced from time to time), and the Swiss Federal Data Protection and Information Commissioner; and

(b) In Clause 17 (Governing Law) the laws of Switzerland shall govern, and in Clause 18 (Choice of forum and jurisdiction) the courts of Switzerland shall have jurisdiction.

5. United Kingdom Law Provisions

5.1 Personal data transfers from the United Kingdom will be governed by the SCCs as conformed to UK law pursuant to the International Data Transfer Addendum (the "IDTA") issued by the UK Information Commissioner's Office (the "ICO") and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022.

5.2 In Part 1 of the IDTA, the information required by Tables 1 – 3 is provided in the Agreement, the DPA and these SCCs.

5.3 The IDTA's Mandatory Clauses are incorporated by reference into this DPA in accordance with IDTA Alternative Part 2.

5.4 References to the EU, member states and GDPR in the SCCs are amended *mutatis mutandis* to refer to the United Kingdom and UK GDPR.

5.5 In Clause 17 of the SCCs (Governing Law), the laws of England and Wales shall govern, and in Clause 18 (Choice of forum and jurisdiction), the courts in London, England shall have jurisdiction. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts in the UK.

6. Supplementary Measures. The following additional safeguards will be added as a new supplementary annex of the EU SCCs:

6.1 Uniform represents that, to the best of its knowledge, as of the Effective Date, it has not received any access requests under Section 702 of the U.S. Foreign Intelligence Surveillance; and

6.2 Uniform will use reasonable measures to encrypt personal data transferred to it pursuant to EU SCCs during transmission.

Annex 1 – Identification of Parties

The full name, address and contact details for the Data Exporter and Data Importer (as defined below) are set out in the Agreement; and

a. In the case of Module 2, Customer and its relevant affiliates which are established in the EEA are the data exporter and controller, and Uniform and its relevant subprocessor affiliates located in non-adequacy approved third countries are the data importer and processor;

b. In the case of Module 3, Customer and its relevant affiliates established in the EEA are the data exporter and processor, and Uniform and its relevant subprocessor affiliates located in non-adequacy approved third countries are the data importer and processor.

Description of Data Processing

The data processing activities carried out by Uniform under the Agreement may be described as follows:

Subject Matter and Purpose

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

Uniform will process Customer personal data in order to perform the Services described in the Agreement. The frequency and retention periods for which personal data may be stored will vary depending on Customer's use of Uniform's Service.

Uniform may process personal data of Customer's employees and consultants who use Uniform's Service in order to improve its own service and user experience by analyzing the usage of its products and providing personalized educational and information materials.

Uniform may have access and process personal data of individuals whose personal data is stored in Customer's data sources as a core functionality of the Uniform product. For example, Uniform may compute data quality metrics based on such data and detect anomalies.

Data subjects

The personal data transferred concern the following categories of data subjects:

Customer's employees and consultants who use Uniform's Service.

Individuals whose personal data is stored in Customer's data sources and processed by Uniform.

Categories of personal data

The personal data transferred concern the following categories of data:

Uniform may have access to personal data of Customer's employees and consultants who use Uniform's Service.

Uniform may have access to personal data of individuals whose personal data is stored in Customer's data sources.

The types of personal data processed are determined by Customer and may include without limitation: Name, Email address, Physical address, IP-address and other online identifiers, Date of birth, Telephone/mobile number, Location Data.

Special categories of data

The personal data transferred concern the following special categories of data:

As above

Annex 2 - Security Measures

Uniform will:

1. take all reasonable measures to prevent unauthorized access to the Data through the use of appropriate physical and logical (passwords) entry controls

2. use built-in system and audit trails;

3. use secure passwords, network intrusion detection technology, encryption and authentication technology, secure login procedures, and virus protection;

4. account for all risks presented by processing, for example, from an accidental or unlawful destruction, loss, or alteration, unauthorized or unlawful storage, processing, access, or disclosure of the Data;

5. ensure pseudonymization and/or encryption of the Data where appropriate;

6. maintain the ability to ensure ongoing confidentiality, integrity, availability, and resilience of processing systems and Services;

7. maintain the ability to restore the availability and access to the Data in a timely manner in the event of a physical or technical incident;

8. implement a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing of the Data;

9. monitor compliance on an ongoing basis;

10. implement measures to identify vulnerabilities concerning the processing of the Data in systems used to provide Services to Customer;

11. provide employee and contractor training to ensure ongoing capabilities to carry out the security measures established in policy.