# TERMLY'S DATA PROCESSING AGREEMENT

This Data Processing DPA (**"DPA"**) forms part of Termly's Terms of Use (the **"Terms"**) between Termly Inc. (**"Termly"**) and the entity identified as the customer below (**"Customer"**). This DPA is supplemental to the Terms and sets out the roles and obligations that apply when Termly processes Personal Data on behalf of Customer in connection with Customer's use of Termly's services ("**Services"**), including in connection with: (a) the generation of policies, legal agreements, disclaimers, and other documents generated by the Services using information related to Customer's business or organization; (b) the management of cookie consent for Customer's website, mobile application, platform and/or digital media (**"Customer's Platform"**); and (c) the management of "Do Not Sell My Information" and other DSAR forms provided to visitors and users of Customer's Platform (**"End Users"**). If there is any conflict between the Terms and this DPA, the terms of this DPA shall prevail to the extent of such conflict. Any capitalized terms not defined in this DPA shall have the meanings given to them in the Terms.

1. Definitions. For the purposes of this DPA:

   a. **"Data Protection Law"** means all data protection and privacy laws and regulations applicable to the processing of Covered Data, including (but not limited to) UK and European Data Protection Law and the California Consumer Privacy Act of 2018 (California Civil Code §§ 1798.100 et seq.) and its implementing regulations (together, the **"CCPA"**).

   b. **"Covered Data"** means the Personal Data that Termly processes on behalf of Customer in connection with the Services, including Personal Data relating to visitors to and users of Customer's Platform (**"End Users"**) that Termly collects in connection with the Services.

   c. **"Customer's Platform"** means the website, mobile application, platform and/or digital media property owned or operated by Customer and via which Covered Data is collected and processed by Termly.

   d. **"Europe"** means, for the purposes of this DPA, the member states of the European Economic Area plus Switzerland and the United Kingdom.

   e. **"UK and European Data Protection Law"** means all data protection and privacy laws and regulations enacted in Europe applicable to the processing of Covered Data, including (but not limited to) (i) Regulation (EU) 2016/679 (the **"GDPR"**); (ii) Directive 2002/58/EC (the **"e-Privacy Directive"**); (iii) the GDPR as it forms part of UK law by virtue of Section 3 of the European Union (Withdrawal) Act 2018 (**"UK GDPR"**); (iv) the UK Data Protection Act 2018 and the UK Privacy and Electronic Communications Regulations 2003, (v) all other applicable EEA and/or UK laws and regulations relating to the processing of personal data and privacy. and (vi) the Swiss Federal Data Protection Act of 19 June 1992 and its corresponding ordinances ("**Swiss DPA**"); in each case, as may be amended, superseded, expanded or replaced from time to time.

   f. **"Personal Data"** means any information that relates to an identified or identifiable natural person and which is protected as "personal data", "personal information" or "personally identifiable information" under Data Protection Law.

   g. "**Security Incident**" means any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Covered Data. "Security Incident" shall not include unsuccessful attempts or activities that do not compromise the security of Covered Data,
   including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

h. **"SCCs"** means the standard contractual clauses annexed to the European Commission's Decision (EU) 2021/914 of 4 June 2021, as described at Section 12 and as may be amended, superseded or replaced.

i. The terms **"controller"**, **"processor"** and **"processing"** shall have the meanings given to them in the GDPR, and **"process"**, **"processes"** and **"processed"** shall be interpreted accordingly; and the terms **"business"**, **"service provider"** and **"consumer"** shall have the meanings given to them in the CCPA.

j "UK Standard Contractual Clauses" or "UK SCCs" means the EU SCCs (as applicable) approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 as amended by the UK Agreement to the EU Standard Contractual Clauses" ("UK Addendum") issued by the Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018 as reproduced at Schedule 7 (UK Addendum).

2. <u>Scope of DPA</u>. This DPA applies to the extent that Termly collects and processes Covered Data on behalf of Customer in connection with the Services, as more particularly described in **Annex 1** (**"Data Processing Description"**).

3. <u>Roles of the parties</u>. As between Termly and Customer, Customer is the controller of Covered Data and Termly shall process the Covered Data as a processor (or service provider) acting on behalf of Customer.

4. <u>Termly's processing of Covered Data.</u> Termly shall process Covered Data in accordance with the lawful, documented instructions of Customer (as set out in the Terms, this DPA or otherwise in writing) and solely for the purposes of providing the Services, including (without limitation) (a) generating and hosting any policies, legal agreements, disclaimers, and other documents generated by the Services; (b) managing End Users' cookie preferences; (c) managing End Users' subject's "Do Not Sell My Information" and DSAR requests; (e) providing and improving Termly's software and products (collectively, the **"Permitted Purposes"**). Termly agrees that it shall not, except to the extent required under applicable law, retain, use, or disclose Covered Data for any purposes other than for the Permitted Purposes or sell Covered Data to a third party for monetary or other valuable consideration within the meaning of the CCPA or otherwise.

5. <u>Customer responsibilities.</u> Customer shall be responsible for complying with all necessary transparency and lawfulness requirements under Data Protection Law in order for Termly to collect and process Covered Data for the Permitted Purposes. Without limiting the generality of the foregoing, Customer acknowledges and agrees that Termly will use certain tracking technologies (including cookies) to collect and process data from End User devices through the Cookie Consent Manager and Customer represents and warrants that it shall provide and maintain all notices and (where applicable) obtain all necessary consents required by Data Protection Law to enable Termly to deploy such tracking technologies lawfully. Termly shall provide all information reasonably requested by Customer (including details about the tracking technologies it serves) to enable Customer to satisfy provide such notice and (where applicable) obtain such consents.

6. <u>Security.</u> Termly shall implement appropriate technical and organisational measures to protect Covered Data from Security Incidents, including as described in **Annex 2** (**"Security Measures"**). Termly may update or modify the Security Measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Services. Termly shall ensure that any personnel that it authorizes to process Covered Data are subject to a duty of confidentiality.

7. Security Incidents. Termly shall notify Customer without undue delay upon becoming aware of a Security Incident. Termly shall make reasonable efforts to identify the cause of the Security Incident and take such steps as Termly deems necessary and reasonable to mitigate the effects of the Security Incident. Termly shall make reasonable efforts to provide such information as Customer may reasonably require to enable Customer to fulfil any data breach reporting obligations under Data Protection Law.

8. Audits. Termly shall make all information available to Customer that is reasonably necessary to verify Termly's compliance with this DPA, including (on a confidential basis) a summary copy of its most recent third party certifications or audit report(s). Termly shall also permit Customer (or its appointed third party auditors) to carry out an audit of Termly's processing under this DPA following a confirmed Security Incident or upon the instruction of a data protection authority. Customer must, where possible, give Termly reasonable prior notice of such intention to audit, conduct its audit during normal business hours and take all reasonable measures to prevent unnecessary disruption to Termly's operations. Customer shall exercise its rights under Clauses 8.9 of the SCCs by instructing Termly to comply with the audit measures described in this Section 8.

9. International transfers. In order to provide the Services, Termly may transfer (directly or via onward transfer) Covered Data to the United States and other locations where Termly or its Sub-processors maintain data processing operations.

10. Data subject rights. Termly shall, taking into account the nature of the processing, provide reasonable assistance to Customer insofar as this is possible, to enable Customer to respond to requests from data subjects seeking to exercise their rights under Data Protection Law.

11. Deletion/return of data. Upon termination or expiry of the Terms, Termly shall delete or return to Customer the Covered Data (including copies) in its possession. This requirement shall not apply to the extent that Termly is required by applicable law to retain some or all of the Covered Data or to Covered Data archived on backup systems, which Termly shall (where reasonably possible) delete within 12 months of termination or expiry of the Terms.

12. European and UK terms. The following terms apply to the extent the Covered Data is subject to UK and European Data Protection Law:

a. Sub-processors. Customer agrees that Termly may engage third party processors (**"Sub-processors"**) to process Covered Data on Termly's behalf, including Termly's current Sub-processors listed at **Annex 3** (**"List of Sub-processors"**), provided that Termly shall (a) maintain an up-to-date list of Sub-processors and make such list available to Customer on request; (b) impose on Sub-processors data protection terms that offer at least the same level of protection for Covered Data as required by this DPA; (c) remain liable for any breach of the DPA caused by its Sub-processors; and (d) provide Customer with ten (10) days' notice of any changes to its Sub-processors. For the avoidance of doubt, Sub-processors shall not include Termly employees or contractors. The parties agree and acknowledge that by complying with this sub-section

(a), Termly fulfils its obligations under Sections 9(a) and (b) of the SCCs, and that Termly may be restricted from disclosing Sub-processor agreements under Clause 9(c) of the SCCs but shall use reasonable efforts to require any Sub-processor it appoints to permit it to disclose the Sub-processor agreement and shall provide (on a confidential basis) all information it reasonably can.

b. Objection to Sub-processors. Customer may object to Termly's engagement of a Sub-processor within five (5) days of receiving notice provided that such objection is based on reasonable grounds relating to data protection. The parties shall cooperate in good faith to reach a resolution and, if such resolution cannot be reached, then Termly may either not engage the Sub-processor or Customer will be permitted to suspend or terminate the processing of Covered Data by Termly (without prejudice to any fees incurred by Customer prior to suspension or termination).

c. International data transfers: For any Personal Data originating in the EEA or the UK to the extent that the processing of this Covered Data is a Restricted Transfer, the parties shall continue to apply the requirements of the GDPR to such data irrespective of the location of processing, and shall ensure a valid legal framework applies for the cross-border transfer of the Personal Data. If another framework, such as the EU-US Transatlantic Privacy Framework (or any other similar program aimed at replacing the now defunct EU-US Privacy Shield) or an adequacy decision under GDPR Art. 45, is not applicable, then Customer and Termly agree that with respect to such Restricted Transfer, and as required by UK and UK and European Data Protection Law, the processing of Covered Data shall be subject to the Standard Contractual Clauses which will apply and form part of the Agreement as follows:

In relation to Covered Data in relation to individuals in the EEA, the EU SCCs will apply completed as follows:

1. Module Two will apply;

2. in Clause 7, the optional docking clause will apply;

3. in Clause 11, the optional language will not apply;

4. in Clause 17, Option 1 will apply, and the EU SCCs will be governed by the laws of the Netherlands;

5. in Clause 18(b), disputes shall be resolved before the courts of Amsterdam, The Netherlands;

6. Annex I of the EU SCCs shall be deemed completed with the information set out in Schedule 1 to this DPA; and

7. Annex II of the EU SCCs shall be deemed completed with the information set out in Schedule 6 to this DPA.

ii. in relation to Covered Data that relates to individuals in the UK, the UK SCCs will apply completed as follows:

1. For so long as it is lawfully permitted to rely on standard contractual clauses for the transfer of Covered Data to controllers set out in the European Commission’s Decision 2010/87/EC of 5 February 2010 (“Prior C2P SCCs”) for transfers of personal data from the United Kingdom, the Prior C2C SCCs shall apply between Termly and Customer on the following basis:

a. Appendix 1 shall be completed with the relevant information set out in Annex 4 to this DPA; and

b. the optional illustrative indemnification Clause will not apply.

iii. Where sub-clause 3(f)(ii)(1) above does not apply and/or Termly and Customer are lawfully permitted to rely on the UK SCCs for transfers of Personal Data from the UK , then:

a. The EU SCCs, completed as set out above in clause 3(f)(i) of this DPA shall apply to transfers of such Covered Data, subject to sub-clause (b) below; and

b. The UK Addendum set out in Schedule 7 shall be deemed executed between the parties and the EU SCCs shall be deemed amended as specified by the UK Addendum in respect of the transfer of such Covered Data.

iv. If neither sub-clause 3(f)(ii)(1)(a) or sub-clause 3(f)(ii)(1)(b) applies, then Termly and Customer shall cooperate in good faith to implement appropriate safeguards for transfers of such Covered Data as required or permitted by the UK GDPR without undue delay.

v. In the event that any provision of this DPA and/or the Agreement(s) contradicts, directly or indirectly, the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail. Each party acknowledges and agrees that any liability owed by one party to the other party under the Standard Contractual Clauses shall at all times be subject to the limitations and exclusions of liability set out in the Agreement.

vi. In furtherance of its obligations as data exporter, Termly may implement and require the Customer to implement reasonable implementation measures that are applicable to Covered Data that is subject to a International data transfer under and subject to this section.

d. Data protection impact assessments. Termly shall, taking into account the nature of the processing and the information available to it, provide reasonable assistance needed to fulfil Customer's obligation to carry out data protection impact assessments and prior consultations with supervisory authorities, to the extent required under UK and European Data Protection Law.

13. Changes in law. In the event of a change in Data Protection Law affecting the processing of Covered Data under this DPA the parties shall work together in good faith to make any amendments to this DPA or to execute any additional written agreements as are reasonably necessary to ensure continued compliance with Data Protection Law. Each party acknowledges that this DPA and any privacy-related provisions in the Terms (with any commercially sensitive information redacted) may be shared with the U.S. Department of Commerce or European regulator on request.

14. Miscellaneous. Except as amended by this DPA, the Terms will remain in full force and effect. If there is a conflict between this DPA and the Terms, the DPA will control. Any claims brought under this DPA shall be subject to the Terms, including but not limited to the exclusions and limitations of liability set forth in the Terms.

IN WITNESS WHEREOF, the parties have caused this DPA to be executed by their authorized representative and this DPA shall be effective on the date both parties sign this DPA:

**Termly Inc.**

Signature:

Name: Da David Reynier

Title: Chief Executive Officer

Date: 2024-01-26

**Customer:** Upfiv Designs Inc.

Signature:

Name: Aurelia McConnell

Title: CEO

Date: 2025-04-30

## Annex 1: Data Processing Description

This **Annex 1** forms part of the DPA and describes the processing that Termly will perform on behalf of Customer.

### 1(A): List of parties

| Data Exporter: | |
|---|---|
| Name: | |
| Address: | |
| Contact person's name, position and contact details: | |
| DPO name and contact details (where applicable): | |
| EU/UK/Switzerland name and contact details (where applicable): | |
| Activities relevant to data transferred under these Clauses: | Provision of the Services under the Agreement |
| Role (controller / processor): | Controller |

| Data Importer: | |
|---|---|
| Name: | Termly Inc |
| Address: | 8 The Grn Ste B Dover, DE 19901 , United States |
| Contact person's name, position and contact details: | David Reynier<br>Chief Executive Officer<br>david@termly.io |
| DPO name and contact details (where applicable): | Masha Komnenic<br>privacy@termly.io |
| EU/UK/Switzerland representative name and contact details (where applicable): | Prighter<br>https://prighter.com/cc/termly |
| Activities relevant to data transferred under these Clauses: | Provision of the Services under the Agreement |
| Role (controller / processor): | Processor |

**1(B): Description of transfer**

| Description | Purpose |
|---|---|
| Categories of data subjects: | End users of Customer's Platform whose Personal data is collected via the Cookie Consent Manager or via DSAR form ("End Users").<br>Customer contacts at Customer’s business or organization (e.g., Customer’s DPO, EU/UK rep, etc.) (“Customer Contacts”) |
| Categories of Personal data: | Form Generator:<br>· Customer Contact name<br>· Customer Contact email<br>· Customer Contact phone number<br>Cookie Consent Manager:<br>· IP address<br>· Country<br>· Cookie preferences<br>· Device type<br>· Time visited<br>· Time preferences where selected<br>DSAR Form Submission:<br>· Customer ID<br>· Website ID<br>· Data Subject Name<br>· Data Subject Email<br>· Access Request (any information submitted on the DSAR form such as request type, agent requesting, relevant law, etc.)<br>· Time submitted |
| Sensitive data transferred (if applicable) and applied restrictions or safeguards: | N/A |
| Frequency of the transfer: | Continuous |
| Subject matter and nature of the processing: | Collection and processing of Personal data relating to Customer Contacts and End Users in connection with the Form Generator, Cookie Consent Manager and DSAR Form Submission. |
| Purpose(s) of the data transfer and further processing: | Processing for the purposes of providing the Services and following Customer's instructions, including (without limitation) (a) providing the form generator and hosting policies, legal agreements, disclaimers, and other documents generated by the Services; (b) providing the Cookie Consent Manager and managing and honoring End Users' cookie preferences; (c) providing the DSAR service and processing End Users' rights requests; (d) generating reporting information relating to the Cookie Consent Manager and DSAR Form Submission; and (e) providing and improving Termly's software and products. |
| Period for which the Personal data will be retained, or, if that is not possible, the criteria used to determine that period: | For the duration of the Terms. |

## Annex 2: Technical and Organizational Security Measures

This **Annex 2** forms part of the DPA and describes the minimum technical and organizational measures implemented by Termly to protect Covered Data from Security Incidents:

1. Measures of pseudonymization and encryption of personal data:
   a. Encryption at rest using an industry standard AES-256 encryption algorithm
   b. Encryption in transit using Transport Layer Security 1.2 (TLS) with an industry-standard AES-256 cipher
2. Measures for ensuring ongoing confidentiality, integrity, availability, and resilience of processing systems and services:
   a. Virtual Private Network (VPN) and Multi-Factor Authentication (MFA) to access Termly cloud data centers
   b. Differentiated rights system based on security groups and access control lists.
   c. Secure transmission of credentials using TLS 1.2 (or greater)
   d. Use of approved password management software.
   e. Guidelines for handling passwords.
   f. Passwords require a defined minimum complexity.
   g. Hashed passwords.
   h. Automatic account locking.
   i. Access controls to infrastructure that is hosted by cloud service provider
   j. Access right management including implementation of access restrictions and managing of individual access rights.
   k. Training for employees and contractors.
   l. Network separation
   m. Segregation of responsibilities and duties
   n. Secure network interconnections ensured by firewalls etc.
   o. Logging of transmissions of data from IT systems that store personal data.
   p. Logging authentication and monitored logical system access
   q. Logging of data access including, but not limited to access, modification, entry and deletion of data
   r. Documentation of data entry rights and logging security related entries
   s. Customer data is backed up to multiple durable data stores in offsite data centers.
   u. Role based access on a need to know basis for employees. Only a few designated employees have access to the infrastructure.
3. Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident:
   a. Termly's cloud service provider provides Distributed Denial of Service (DDoS) protection services that safeguards applications on Termly Servers including always-on detection and automatic inline mitigations that minimize application downtime and latency.
   b. Termly's data backups are conducted on Termly's cloud service provider's offsite data centers.
   c. Data is backed up to multiple durable data stores in offsite data centers.
   d. All data is backed up hourly in incremental segments and daily as a full backup. All backups are kept redundant and in encrypted form (AES-256).
   e. Procedures for handling and reporting incidents (incident management) including the detection and reaction to possible security incidents.
4. Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing
   a. Security checks (e.g., penetration tests) conducted by external parties.
   b. Regular network and application security testing via cloud service provider.
   c. Testing emergency equipment via Termly's cloud service provider.
5. Measures for user identification and authorisation:
   a. Access to data necessary for the performance of the particular task is ensured within the systems and applications by corresponding identity access management and authorization concept.
   b. Virtual Private Network (VPN) and Multi-Factor Authentication (MFA) to access Termly data centers.
   c. Secure network interconnections ensured by VPN, MFA, firewalls etc.

   d. Logging of transmissions of data from IT system that stores or processes personal data
   e. Logging authentication and monitored system access.

6. Measures for the protection of data during transmission
    a. Encryption in transit using Transport Layer Security 1.2 (TLS) with an industry-standard AES-256 cipher.
    b. Remote access to the network via VPN tunnel and end-to-end encryption.
7. Measures for the protection of data during storage
    a. Encryption at rest using an industry standard AES-256 encryption algorithm.
    b. Virtual Private Network (VPN) and Multi-Factor Authentication (MFA) to access data centers.
    c. Use of Access Control Lists.
8. Measures for ensuring physical security of locations at which personal data are processed
    a. Cloud service provider implements physical and environmental controls such as secure design (site selection, redundancy, availability, and capacity planning), business continuity & disaster recovery (business continuity plan, pandemic response), physical access controls, monitoring and logging (data center access review, logs, and monitoring), surveillance and detection (CCTV, data center entry points, intrusion detection), device management (asset management, media destruction), operational support systems (power, climate and temperature, fire detection and suppression, leakage detection), infrastructure maintenance (equipment maintenance, environment management), and governance & risk (ongoing data center risk management, security attestation)

9. Measures for ensuring events logging
    a. Cloud service provider enables logging on accounts and records account activity from account creation.
    b. Cloud service provider uses methods like the following to ensure the verifiability of event log files: remote logging, hash chaining, repliciation, Central Security Event and Information Management (SIEM) system.
10. Measures for ensuring system configuration, including default configuration
    a. System configuration from the source code that is predetermined per Application/Infrastructure as Code (IaC)
    b. Access Control Policy and Procedures
    c. Baseline configuration identification
    d. Configuration Planning and Management
11. Measures for internal IT and IT security governance and management
    a. Dedicated and identified person to oversee the company's information security and compliance program
12. Measures for ensuring data minimisation
    a. Privacy by design/default (privacy impact assessment process)
13. Measures for ensuring data quality
    a. Process for the exercise of data protection rights (right to amend and update information).
14. Measures for ensuring limited data retention
    a. Annual review of data retention policy and processes
    b. Operational mechanisms to ensure deletion (e.g., automatic deletion of data after a predefined time period)
15. Measures for ensuring accountability
    a. Assigned responsibility to ensure end-user privacy throughout the product lifecycle and through applicable business processes.
    b. Data protection impact assessments as an integral part of any new processing initiative.
16. Measures for allowing data portability and ensuring erasure
    a. Documented processes in relation to the exercise by users of their privacy rights (e.g. right of erasure or right to data portability)

b. Use of open formats such as CSV, XML or JSON.17. Measures for ensuring secure Third-Party processing
In order for us to provide our customers with the Service in accordance with our DPA, we maintain contractual relationships with vendors. This includes contractual agreements, privacy policies, and vendor compliance programs. Vendors are vetted for privacy and security compliance during the vendor assessment process.

## Annex 3: List of Sub-processors

This **Annex 3** forms part of the DPA and describes Termly's current sub-processors.

| **Name** | **Address:** | **Description of processing:** | **Types of personal data:** |
|---|---|---|---|
| Amazon Web Services, Inc. | USA, California | Hosting | Customers and End Users:<br>- contact information<br>- device information<br>- commercial information<br>- IP addresses |
| BigQuery | USA, California | Combines data to create summary of user actions | Customers and End Users:<br>- device information<br>- usage data<br>- commercial information<br>- IP addresses |
| Cloudflare, Inc. | USA, California | Proxy server | Customers and End Users:<br>- device information<br>- logins<br>- IP addresses |
| Datadog | USA, New York | Application performance, metrics aggregation, displaying data and alerting | Customers and End Users:<br>- contact information<br>- device information<br>- commercial information<br>- IP addresses |
| Looker Studio | USA, California | Combines data to create summary of user actions | Customers and End Users:<br>- device information<br>- usage data<br>- IP addresses |
| Heap | USA, California | Analyze user behavior | Customers and End Users:<br>- device information<br>- usage data<br>- commercial information<br>- IP addresses |
| Hubspot | USA, California | Customer Relationship Management | Customers and End Users:<br>- contact information<br>- commercial information<br>- communication content |

| | | | |
|---|---|---|---|
| Intercom | USA, California | Customer Support AI chatbots | Customers and End Users:<br>- contact information<br>- device information<br>- commercial information<br>- communication content |
| Microsoft 365 Exchange Online | USA, Washington | Email hosting and mail services | Customers and End Users:<br>- contact information<br>- communication content<br>- email data<br>- calendar data |
| Microsoft Entra | USA, Washington | SSO and identity provider | Customers and End Users:<br>- login credentials<br>- IP addresses<br>- authentication logs<br>- device information |
| Microsoft SharePoint/OneDrive | USA, Washington | File storage and collaboration | Customers and End Users:<br>- contact information<br>- collaboration content<br>- file data<br>- sharing permissions |
| Microsoft Teams | USA, Washington | Team communication and video conferencing | Customers and End Users:<br>- contact information<br>- communication content<br>- meeting recordings<br>- chat data |
| SendGrid, Inc. | USA, California | Email communication for DSAR, product updates | Customers and End Users:<br>- contact information<br>- commercial information<br>- communication content |
| Retool | USA, California | Internal dashboard centralizing customer information across our tools, to improve our Customer Service. | Customers and End Users:<br>- contact information<br>- device information<br>- commercial information<br>- communication content |

| | | | |
|---|---|---|---|
| Sentry | USA, California | Error monitoring | Customers and End Users:<br>- contact information<br>- device information<br>- commercial information<br>- IP addresses |
| Stripe | Dublin, Ireland | Payments and refunds processing | Customers and End Users:<br>- contact information<br>- commercial information<br>- financial information |
| Userflow | USA, California | Product onboarding and user guidance | Customers and End Users:<br>- usage data<br>- UI interaction data<br>- IP addresses |
| Zendesk | USA, California | Customer support platform | Customers and End Users:<br>- contact information<br>- support tickets<br>- communication content<br>- device information |

## Annex 4: UK addendum

| UK Controller to Processor SCCs | |
|---|---|
| References to the relevant clauses, which together form the UK | Module 2 of the EEA Standard Contractual Clauses, including any relevant appendices and clauses set out in this UK Addendum, save as modified or amended as set out below and including Part 2: Mandatory Clauses of the Approved Addendum, being the template addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022 as it is revised under Section 18 of those Mandatory Clauses. |
| Standard Contractual Clauses | The parties agree that Clause 7 shall apply. |
| Optional Clause 7 (Docking Clause) | Option 2: General Written Authorisation |
| Clause 9 (a) options (use of subprocessors) | The parties specify the time period as follows: 30 days |
| Optional Clause 11(a) (Redress) | The optional clause under Clause 11 (a) shall not apply. |
| Optional Clause 13(a) (competent supervisory authority) | The competent Supervisory Authority shall be the UK Information Commissioner's Office. |
| Clause 17 (Governing Law): for the purposes of Clause 17 the Parties agree that the governing law shall be as follows. | English law |
| Clause 18 (Courts): for the purposes of Clause 18 paragraph (b) the parties agree that any dispute shall be resolved by: | Courts of England and Wales |
| Annex 1A: List of parties | As set out in the DPA |
| Annex 1B: Description of Transfer | As described in the DPA |
| Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data | As described in the DPA |
| Annex III: List of Subprocessors | As described in the DPA |
| Which parties may end the UK Addendum as set out in Section 19 of the UK Addendum | As set out in the DPA |