Consent Pro | by {Finsweet

Last Updated: September 17, 2026

Data Processing Agreement

Finsweet Inc. ("**Finsweet**" or "**Company**") and the entity agreeing to these terms ("**Customer**") have entered into an agreement governing Customer's use of Consent Pro (the "**Agreement**"). This Data Processing Addendum, including its Exhibits (the "**DPA**"), forms part of the Agreement and applies to Finsweet's processing of Personal Data in connection with the Consent Pro service.

This DPA is effective from, and supersedes any previously applicable data processing terms relating to Consent Pro from, the date on which Customer accepted the Agreement or otherwise agreed to this DPA (the "**DPA Effective Date**").

If you are accepting this DPA on behalf of Customer, you warrant that (a) you have full legal authority to bind Customer to this DPA, (b) you have read and understand this DPA, and (c) you agree, on behalf of Customer, to this DPA. If you do not have that authority, do not accept this DPA.

1. Definitions

1.1 Terms used in this DPA have the meanings below. Capitalised terms not defined here have the meaning given in the Agreement.

"Affiliate" means an entity that directly or indirectly controls, is controlled by, or is under common control with a party, where "control" means ownership of more than fifty percent (50%) of the voting equity, for so long as such control exists.

"Applicable Data Protection Laws" means all laws and regulations applicable to the processing of Personal Data under the Agreement, including European Data Protection Laws and US State Privacy Laws.

"Authorised Sub-Processor" means a third party engaged by Finsweet to process Personal Data in connection with the Services, as listed at https://trust.finsweet.com/subprocessors or subsequently authorised under Section 5.

"Company Account Data" means Personal Data relating to Finsweet's commercial relationship with Customer, including the names and contact details of individuals authorised to access Customer's Consent Pro account, billing contacts, and data collected for identity verification, fraud prevention, or as required by applicable law.

"Company Usage Data" means service telemetry generated by Finsweet in connection with the operation of the Services, including activity and error logs, performance data, and data used to detect and prevent abuse of the Services.

"Consent Data" means Personal Data captured, stored, and made available by the Services that records the consent, refusal, or preference choices of an End User, together with the technical and contextual metadata associated with each such record, as further described in Exhibit A.

“Consent Pro” or the **“Services”** means Finsweet’s consent management platform, comprising the consent banner and preference interface deployed on Customer’s Digital Properties, the consent record store, the tracking technology scanner, the policy document generator, and the associated dashboard and APIs.

“Data Privacy Framework” or **“DPF”** means the EU–U.S. Data Privacy Framework, the UK Extension to the EU–U.S. Data Privacy Framework, and the Swiss–U.S. Data Privacy Framework, as administered by the U.S. Department of Commerce.

“Digital Properties” means the websites, applications, and other online properties owned or operated by Customer on which the Services are deployed.

“End User” means a natural person who visits or interacts with a Digital Property and whose consent choices are captured or processed by the Services.

“EU SCCs” means the standard contractual clauses annexed to European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as amended or replaced from time to time.

“European Data Protection Laws” means (i) Regulation (EU) 2016/679 (the “**EU GDPR**”); (ii) the EU GDPR as retained in the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018, together with the Data Protection Act 2018 (the “**UK GDPR**”); (iii) the Swiss Federal Act on Data Protection of 25 September 2020, which entered into force on 1 September 2023, and its implementing ordinances (the “**Swiss FADP**”); (iv) Directive 2002/58/EC (the “**ePrivacy Directive**”) and its national implementations, including the Privacy and Electronic Communications (EC Directive) Regulations 2003; and (v) any national data protection laws made under or applying in conjunction with the foregoing.

“Opt-Out Preference Signal” means a signal transmitted by an End User’s browser, device, or other user agent communicating a choice to opt out of the sale or sharing of personal information or of targeted advertising, including the Global Privacy Control.

“Personal Data” means any information falling within the definition of “personal data,” “personal information,” or “personally identifiable information” under Applicable Data Protection Laws that is processed by Finsweet in connection with the Services.

“Personal Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of or access to Personal Data processed by Finsweet in connection with the Services.

“Restricted Transfer” means a transfer of Personal Data protected by European Data Protection Laws to a country that is not the subject of an adequacy decision or adequacy regulations under the applicable European Data Protection Law.

“UK Addendum” means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (Version B1.0) issued by the Information Commissioner’s Office under s.119A of the Data Protection Act 2018.

“US State Privacy Laws” means all comprehensive state privacy laws of the United States applicable to the processing of Personal Data under the Agreement, including the California Consumer Privacy Act of 2018 as amended by the California Privacy Rights Act of 2020 and its

implementing regulations (the "**CCPA**"), and the comprehensive consumer privacy statutes of Virginia, Colorado, Connecticut, Utah, Texas, Oregon, Montana, Florida, Delaware, Iowa, Nebraska, New Hampshire, New Jersey, Tennessee, Minnesota, Maryland, Kentucky, Rhode Island, and Indiana, in each case as and when effective and as amended or replaced from time to time.

1.2 The terms "controller," "processor," "data subject," "processing," and "supervisory authority" have the meanings given in European Data Protection Laws. "Business," "service provider," "contractor," "sell," "share," and "sensitive personal information" have the meanings given in the CCPA.

2. Roles of the Parties and Scope

2.1 The subject matter, duration, nature and purpose of the processing, the types of Personal Data, and the categories of data subjects are described in **Exhibit A**.

2.2 With respect to Consent Data and all other Personal Data that Customer or its End Users submit to, or that is collected by, the Services, the parties agree that **Customer is the controller** (or, where Customer processes such Personal Data on behalf of a third party, a processor) and **Finsweet is a processor** (or sub-processor, as applicable).

2.3 With respect to Company Account Data and Company Usage Data, Finsweet is an **independent controller** and not a joint controller with Customer. Section 12 governs that processing.

2.4 Customer is solely responsible for: (a) the accuracy, quality and lawfulness of Personal Data processed through the Services; (b) establishing and maintaining a valid legal basis for the processing, including for the deployment of the Services and any tracking technologies on its Digital Properties; (c) the configuration of consent purposes, categories, and banner text within the Services; (d) the content and accuracy of any policy document generated by the Services and published on its Digital Properties; and (e) determining whether the Services, as configured by Customer, meet Customer's own compliance obligations.

2.5 Customer acknowledges that the Services provide tooling to support Customer's compliance obligations and that Finsweet does not provide legal advice. Policy documents generated by the Services are produced from inputs supplied by Customer and are Customer's responsibility to review.

3. Processing Instructions

3.1 With respect to Personal Data Finsweet processes on Customer's behalf under Section 2.2, Finsweet shall process such Personal Data only:

a) for the limited and specified purpose of providing, securing and maintaining the Services; b) in accordance with Customer's documented instructions as set out in the Agreement, this DPA, and the configuration options Customer selects within the Services; and c) in accordance with Applicable Data Protection Laws.

3.2 Customer’s use of the Services, including its configuration of consent purposes and policy document generation, constitutes documented instructions to Finsweet to process Personal Data accordingly. Where Customer enters the name or contact details of a data protection officer, EU or UK representative, or privacy contact into the policy generation interface, Customer instructs Finsweet to render and publish those details within the resulting policy document on Customer’s Digital Properties.

3.3 Finsweet shall not:

a) retain, use, or disclose Personal Data for any purpose other than performing the Services, or otherwise outside the direct business relationship with Customer, except as permitted by Applicable Data Protection Laws; b) sell or share Personal Data, as those terms are defined under US State Privacy Laws; c) use Personal Data for marketing or advertising purposes, or for cross-context behavioural advertising; or d) combine Personal Data received under this DPA with Personal Data received from or on behalf of any other person, or collected from its own interactions with data subjects, except as permitted by Applicable Data Protection Laws.

3.4 Finsweet shall not process Personal Data to develop, train, or improve any machine learning or artificial intelligence model, except that Finsweet may use aggregated and de-identified data that does not identify Customer, any End User, or any Digital Property to operate and improve the Services.

3.5 Finsweet shall promptly notify Customer if, in Finsweet’s opinion, an instruction from Customer infringes Applicable Data Protection Laws, or if Finsweet determines that it can no longer meet its obligations under Applicable Data Protection Laws. Finsweet shall inform Customer before processing Personal Data where required to do so by law, unless that law prohibits such notification on important grounds of public interest.

3.6 Customer may, upon notice, take reasonable and appropriate steps to stop and remediate any unauthorised use of Personal Data by Finsweet.

4. Consent Data, Opt-Out Preference Signals and Retention

4.1 Integrity of consent records. Finsweet shall maintain each consent record as an append-only entry, save where a Customer's Consent Data is deleted in full under Section 4.4 or Section 8.1, associated with the version of the consent notice and policy template presented to the End User at the time the record was created, so that Customer can evidence what the End User was shown when consent was given, refused, or withdrawn. Finsweet does not correct or edit a consent record once it has been recorded; a subsequent change in an End User's choice is captured by a new consent record, not an alteration of an earlier one.

4.2 Opt-Out Preference Signals. The Services automatically detect the Global Privacy Control signal transmitted by an End User’s user agent and apply it in accordance with Customer’s configuration (including the consent banner mode Customer has selected) and Applicable Data Protection Laws. There is no setting by which Customer can disable detection of the signal. Customer acknowledges that current consent records do not capture an indication of whether a Global Privacy Control signal was received or whether it was applied to the choices recorded.

4.3 Retention.

Finsweet's retention policy for Consent Data is five (5) years from each consent record's own date — the date of the consent event it reflects. Where an End User later makes a new choice, that choice is captured as a separate consent record with its own retention period; an earlier record's retention period is not extended or reset by a later one. Finsweet has not yet implemented an automated mechanism to delete Consent Data once this period elapses; until it does, Consent Data is not automatically deleted at the end of the stated retention period, and deletion before then is available only as described in Section 8.1. Customer acknowledges that consent records constitute evidence of consent, and that retention for the period during which Customer relies on that consent, plus any applicable limitation period, may be necessary for the establishment, exercise, or defence of legal claims.

4.4 Deletion and return.

On termination or expiry of the Agreement, and at Customer's choice, Finsweet will delete or return all Personal Data processed by Finsweet on Customer's behalf under this DPA within thirty (30) days of termination or expiry, **and will delete existing copies unless the law requires storage.** Where deletion is prohibited by law, Finsweet shall block the Personal Data from further processing and continue to protect it in accordance with this DPA. Where the parties have entered into the EU SCCs and deletion is selected, Finsweet will certify deletion as required by Clause 8.5.

4.5 Data residency. Consent Data is stored in object storage located in Western Europe. Customer acknowledges that storage of Personal Data within the European Economic Area does not by itself prevent a Restricted Transfer, and that access to that Personal Data by Finsweet personnel located in the United States for the purposes of providing, supporting and securing the Services constitutes a transfer for the purposes of European Data Protection Laws. Section 7 applies to such access.

5. Sub-Processors

5.1 Customer grants Finsweet general written authorisation to engage (a) Finsweet Affiliates and (b) the third parties listed at https://trust.finsweet.com/subprocessors (the "**List**") as Authorised Sub-Processors to process Personal Data in connection with the Services. Where the EU SCCs apply to a transfer under this DPA, the sub-processors relevant to that transfer are separately identified in Exhibit B, Annex III, which reflects only those Authorised Sub-Processors processing Personal Data within the scope of that transfer and is narrower than the List by design.

5.2 Each Authorised Sub-Processor is subject to binding contractual data-protection obligations as required by applicable Data Protection Law and, where applicable, the EU SCCs. Finsweet shall remain liable to Customer for the performance of each Authorised Sub-Processor's obligations, subject to the limitations and exclusions of liability in the Agreement, as provided in Section 14.2 of this DPA.

5.3 Finsweet shall notify Customer in writing (including electronically) of any intended new or replacement Authorised Sub-Processor at least **thirty (30) days** before that sub-processor begins processing Personal Data, and shall add the sub-processor to the List accordingly.

5.4 Customer may object to a new or replacement Authorised Sub-Processor on reasonable grounds relating to data protection by giving written notice within thirty (30) days of Finsweet's notice under Section 5.3. The parties shall seek in good faith to resolve the objection. If Finsweet cannot provide a commercially reasonable alternative within a reasonable period, Customer may terminate the affected Services on written notice. Termination under this Section does not relieve Customer of fees accrued before the termination date.

5.5 Where the parties have entered into the EU SCCs, the authorisation in Section 5.1 constitutes Customer's prior written consent for the purposes of Clause 9, and copies of sub-processor agreements provided under Clause 9(c) may be redacted of commercial terms and provided on request.

6. Security

6.1 Taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing, as well as the risks to data subjects, Finsweet shall implement and maintain the technical and organisational measures described in **Exhibit C**.

6.2 Finsweet shall ensure that all personnel authorised to access Personal Data are bound by contractual or statutory obligations of confidentiality and have received appropriate data protection and security training, provided on at least an annual basis.

6.3 Customer acknowledges that the measures in Exhibit C are subject to technical progress, and that Finsweet may update them provided that no update materially degrades the overall security of the Services.

7. International Transfers

7.1 Consent Data is stored within the European Economic Area as described in Section 4.5. Customer acknowledges that Finsweet is established in the United States and that its personnel access Personal Data from the United States for the purposes of providing, supporting, administering and securing the Services, and that such access constitutes a transfer of Personal Data to a third country. Company Account Data and certain Company Usage Data are processed in the United States.

7.2 Data Privacy Framework. Finsweet is **not** certified under the Data Privacy Framework. All Restricted Transfers under this DPA are made under the EU SCCs, the UK Addendum and the Swiss provisions set out below. Should Finsweet certify to the Data Privacy Framework in future, it shall notify Customer, and the EU SCCs set out in Section 7.3 shall continue to apply in addition to and independently of that certification.

7.3 EU transfers. Where a transfer of Personal Data protected by the EU GDPR is a Restricted Transfer, the Parties adopt the standard contractual clauses approved by the European Commission in Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (OJ L 199, 7.6.2021, p. 31), currently published at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj (the "**EU SCCs**"), in full and without modification except as those Clauses themselves permit — to select the applicable Module(s) and Clause options, and to complete the required Annexes — as follows:

a) **Module Two** (controller to processor) applies where Customer is a controller; **Module Three** (processor to sub-processor) applies where Customer is a processor. **Module One** (controller to controller) applies to Company Account Data and Company Usage Data processed by Finsweet under Section 12; b) in Clause 7, the docking clause does not apply; c) in Clause 9, Option 2 (general written authorisation) applies, with the notice period set out in Section 5.3; d) in Clause 11, the optional language does not apply; e) all square brackets in Clause 13 are removed; f) in Clause 17, Option 1 applies and the EU SCCs are governed by the law of Ireland; g) in Clause 18(b), disputes shall be resolved before the courts of Ireland; h) Annex I and Annex III are completed by **Exhibit B**; Annex II is completed by **Exhibit C**; and i) by accepting this DPA the parties are deemed to have signed the EU SCCs, including their Annexes.

The Clauses of the EU SCCs are incorporated by reference in the form officially published by the European Commission; they are not reproduced in this DPA, and nothing in this DPA modifies their text. If the European Commission revises or replaces the officially published text of the EU SCCs, the revised or replacement text applies between the Parties from the date the Commission specifies.

7.4 UK transfers. Restricted Transfers of Personal Data protected by the UK GDPR are made under the EU SCCs as completed above, as amended by the **UK Addendum** set out in **Exhibit D**.

7.5 Swiss transfers. Restricted Transfers of Personal Data protected by the Swiss FADP are made under the EU SCCs as completed above, with the following modifications: (a) references to the GDPR are understood as references to the Swiss FADP; (b) the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner; (c) references to "Member State" shall not be read so as to prevent data subjects in Switzerland from exercising their rights in their place of habitual residence under Clause 18(c); and (d) in Clause 17 the governing law is the law of Switzerland.

7.6 Onward transfers. Finsweet shall not make, and shall not permit any Authorised Sub-Processor to make, any onward Restricted Transfer of Personal Data except in full compliance with Applicable Data Protection Laws and, where applicable, the EU SCCs and UK Addendum.

7.7 Transfer assessments. Finsweet shall, on request and to the extent able, provide reasonable assistance to Customer in conducting a transfer impact assessment.

7.8 Precedence. In the event of any conflict between this DPA and the EU SCCs or UK Addendum, the EU SCCs or UK Addendum shall prevail.

8. Data Subject Rights

8.1 Taking into account the nature of the processing, Finsweet shall, on Customer's written request, provide access to, or export, Consent Data associated with an End User identified by Customer. Customer is responsible for identifying the relevant records, including by supplying the applicable Consent ID. Consistent with Section 4.1, Finsweet does not correct or edit a consent record once it has been recorded; where Customer has exported Consent Data, or it has been forwarded to a destination Customer controls, any changes Customer makes to that copy are Customer's own and do not alter the record Finsweet maintains. Finsweet does not currently support deletion of an individual End User's Consent Data, a specific End User's records, or a Property's consent logs, through the Services or via API. Where Customer requires such data to be deleted before the

retention period described in Section 4.3 otherwise applies, Finsweet will delete the affected Consent Data as part of a full removal of Customer's data from the Services, carried out manually on Customer's request under Finsweet's existing account-level deletion process.

8.2 If Finsweet receives a request from a data subject to exercise rights of access, rectification, erasure, restriction, portability, objection, withdrawal of consent, or opt-out in respect of Personal Data processed on Customer's behalf, Finsweet shall not respond substantively except to confirm that the request relates to Customer, and shall promptly notify Customer and direct the data subject to Customer.

8.3 Where Customer is unable to respond to such a request using the mechanism in Section 8.1, Finsweet shall provide reasonable assistance, taking into account the nature of the processing. Customer is responsible for verifying the identity of the requester. Customer shall bear reasonable costs of assistance beyond the scope of Section 8.1.

9. Personal Data Breach

9.1 Finsweet shall notify Customer without undue delay, after becoming aware of a Personal Data Breach affecting Personal Data processed on Customer's behalf.

9.2 The notification shall include, to the extent known at the time and supplemented as further information becomes available: the nature of the breach, the categories and approximate number of data subjects and records affected, the likely consequences, and the measures taken or proposed. Finsweet shall not delay initial notification in order to complete its investigation.

9.3 Finsweet shall take reasonable steps to contain, investigate and remediate the Personal Data Breach, and shall provide Customer with reasonable cooperation and assistance in connection with Customer's own notification obligations to supervisory authorities and data subjects.

9.4 Finsweet shall not make any public announcement identifying Customer in connection with a Personal Data Breach without Customer's prior written consent, unless required by law.

9.5 Notification of a Personal Data Breach is not an acknowledgement of fault or liability.

10. Assistance, Records and Audit

10.1 Taking into account the nature of the processing and the information available to it, Finsweet shall provide Customer with reasonable assistance in relation to data protection impact assessments and prior consultations with supervisory authorities, where required by Applicable Data Protection Laws and where Customer does not otherwise have access to the relevant information.

10.2 Finsweet shall maintain records sufficient to demonstrate compliance with this DPA and shall make available to Customer, on written request at reasonable intervals and subject to confidentiality obligations, such information as is reasonably necessary to demonstrate compliance, including its most recent third-party audit reports and certifications.

10.3 Where the information provided under Section 10.2 is, in Customer's reasonable judgement, insufficient to demonstrate compliance, Customer may request an audit, subject to the following: (a) no more than one audit per calendar year, save where required by a supervisory authority or following a Personal Data Breach; (b) at least thirty (30) days' prior written notice; (c) conducted during business hours and in a manner that is not unreasonably disruptive; (d) limited in scope to processing relevant to Customer; and (e) at Customer's cost, including reasonable reimbursement of Finsweet's time.

10.4 Finsweet may object in writing to an auditor appointed by Customer that is a competitor of Finsweet or is not suitably qualified or independent, in which case Customer shall appoint an alternative auditor or conduct the audit itself.

10.5 Where the parties have entered into the EU SCCs, audits under Clause 8.9 shall be carried out in accordance with this Section 10.

11. US State Privacy Laws

11.1 With respect to Personal Data Finsweet processes on Customer's behalf under Section 2.2, to the extent processed within the scope of US State Privacy Laws, Finsweet acts as a **service provider** and, where applicable, a **processor** to Customer as **business** or **controller**, and receives Personal Data solely for the business purpose of providing the Services.

11.2 Finsweet certifies that it understands and shall comply with the restrictions in Section 3.3 and this Section 11.

11.3 Finsweet shall assist Customer in responding to consumer requests to know, delete, correct, opt out of sale or sharing, limit the use of sensitive personal information, and opt out of targeted advertising or profiling, in each case to the extent applicable to the Services. The Services support the Global Privacy Control as an Opt-Out Preference Signal in accordance with Section 4.2.

11.4 Finsweet shall notify Customer without undue delay if it determines that it can no longer meet its obligations under US State Privacy Laws, and shall cooperate with Customer in stopping and remediating any unauthorised use of Personal Data.

11.5 Customer shall not submit, and shall configure the Services so as not to collect sensitive personal information beyond that necessary for the operation of the Services. Finsweet shall not use any sensitive personal information for any purpose other than those permitted under Applicable Data Protection Laws.

12. Finsweet as Controller

12.1 With respect to Company Account Data and Company Usage Data, Finsweet is an independent controller and processes such data to: (a) manage its relationship with Customer; (b) carry out core business operations including accounting, audit, tax and compliance; (c) monitor, investigate, prevent and detect fraud, security incidents and misuse of the Services; (d) verify identity; (e) provide, secure, maintain and improve the Services; and (f) comply with legal obligations to which it is subject.

12.2 Finsweet's processing as a controller is carried out in accordance with the Consent Pro Privacy Policy, available here, which covers Company Account Data and Company Usage Data for individuals worldwide, including those in the EEA, UK and Switzerland.

13. Government and Third-Party Access Requests

13.1 If Finsweet receives a legally binding request from a public authority or third party for disclosure of Personal Data processed on Customer's behalf, Finsweet shall: (a) notify Customer without undue delay unless prohibited by law; (b) inform the requesting party that it is a processor and is not authorised to disclose the Personal Data; (c) direct the requesting party to Customer, disclosing the minimum contact details necessary to do so; and (d) where disclosure is legally compelled, disclose only the minimum Personal Data legally required.

13.2 Finsweet shall challenge any request that it assesses to be unlawful, including by pursuing available legal remedies, and shall not disclose Personal Data until required to do so under applicable procedural rules.

13.3 Finsweet shall not voluntarily disclose Personal Data to any law enforcement or government agency.

13.4 As at the DPA Effective Date, Finsweet has not received any request from a government intelligence or security agency for access to Personal Data processed under this DPA.

14. General

14.1 Precedence. In the event of conflict, the order of precedence is: (1) the EU SCCs and UK Addendum; (2) this DPA; (3) the Agreement; (4) Finsweet's privacy policy.

14.2 Liability. Finsweet's liability under this DPA is subject to the exclusions and limitations of liability in the Agreement, to the maximum extent permitted by applicable law. This Section 14.2 applies notwithstanding Section 14.1 or the Agreement's general rule that this DPA prevails on matters of data protection law. As between Customer and Finsweet, and only to the extent legally permitted and insofar as doing so does not contradict or undermine the liability scheme the EU SCCs establish, this cap may apply to liability between the Parties under Clause 12(a) of the EU SCCs. Nothing in this DPA modifies, restricts, or expressly limits any other liability, right, or mechanism under Clause 12 of the EU SCCs — including a data subject's right to full compensation and the Parties' joint and several liability to a data subject under Clause 12(b), (c) and (e), and the contribution and claim-back mechanisms under Clause 12(d) and (f). Nothing in this DPA limits or excludes either party's liability to data subjects or supervisory authorities, who are not parties to the Agreement.

14.3 Third-party rights. Except as expressly provided in the EU SCCs or required by Applicable Data Protection Laws, this DPA confers no third-party beneficiary rights.

14.4 Governing law. This DPA is governed by the law specified in the Agreement, save where the EU SCCs, UK Addendum, or Swiss provisions specify otherwise.

14.5 Severability. If any provision of this DPA is held invalid or unenforceable, the remaining provisions remain in effect.

14.6 Changes. Finsweet may update this DPA to reflect changes in Applicable Data Protection Laws or the Services, provided that no update materially reduces the protections afforded to Personal Data. Finsweet shall give Customer at least thirty (30) days' notice of any material change.

Exhibit A — Details of Processing

Nature and purpose of processing

Finsweet processes Personal Data as necessary to provide the Consent Pro service, comprising:

- **Consent capture and storage** — presenting a consent notice or preference interface to End Users on Customer's Digital Properties, and recording the resulting choices;
- **Consent retrieval** — making consent state available to Customer's Digital Properties and to Customer's own tag management and analytics tooling at page load;
- **Opt-out preference signal handling** — detecting and applying signals transmitted by an End User's user agent;
- **Tracking technology scanning** — scanning Customer's Digital Properties to inventory cookies and similar technologies for the cookie declaration;
- **Policy document generation** — rendering Privacy Policy, Cookie Policy, Privacy Rights, and Do Not Sell or Share My Personal Information documents from inputs supplied by Customer, for publication on Customer's Digital Properties;
- **Dashboard and administration** — authenticating administrators, and providing reporting, configuration and export functionality;
- **Support, security and service operation** — including hosting, backup, logging, abuse prevention, and technical support.

Processing operations include collection, recording, storage, structuring, retrieval, consultation, use, disclosure to Authorised Sub-Processors, erasure and destruction.

For Company Account Data and Company Usage Data processed by Finsweet as an independent controller, the purposes of processing are those described in Section 12.1.

Categories of data subjects

1. **End Users** — natural persons who visit or interact with Customer's Digital Properties and whose consent choices are captured by the Services.
2. **Administrators** — Customer's employees, consultants, contractors and agents authorised to access the Consent Pro dashboard.
3. **Named contacts in generated policies** — natural persons whose details Customer enters into the policy generation interface, including data protection officers, EU and UK Article 27 representatives, and privacy contacts.

Categories of Personal Data

In relation to End Users — Consent Data:

- A pseudonymous consent identifier stored in a first-party cookie or in browser local storage
- Consent state per purpose category (for example: necessary, analytics, marketing, personalisation), and whether each was granted, refused, or withdrawn
- Timestamp of each consent event, including grant, update and withdrawal
- The method by which consent was expressed (for example: banner accept, banner reject, granular preference selection, implied continuation where permitted)
- The version identifier of the consent notice and policy template presented at the time of the event
- The domain and page URL on which the consent event occurred

The Services do not implement the IAB Transparency and Consent Framework or the IAB Global Privacy Platform, and do not store a TCF or GPP consent string.

In relation to End Users — technical data:

- A pseudonymous user_identifier, derived at the point of consent ingest by applying SHA-256 to the End User's IP address combined with a secret value held by Finsweet, and truncating the result. **The raw IP address is not persisted at any point.** The user_identifier is a pseudonymous identifier and remains Personal Data; it is not anonymous data, because Finsweet holds the secret value necessary to re-derive it.
- Country of origin, derived from the request at the network edge (CF-IPCountry), used to determine the applicable regulatory framework. No finer-grained geolocation is derived or stored.
- User agent string, browser and device type

The consent record identifier is supplied by the client and is not derived from the IP address.

In relation to Administrators:

- Name, email address, and authentication identifiers (managed via Auth0 for the Consent Pro Web App, or a Webflow ID token for administrators accessing through the Webflow Designer Extension App)
- Role and permission assignments
- IP address and dashboard-activity attribution metadata (created-by / updated-by records)

In relation to named contacts in generated policies:

- Company legal name, registered address, country
- Privacy contact email address and telephone number
- Data protection officer name and contact details, where supplied
- EU and UK representative name and contact details, where supplied

Customer acknowledges that the details in this last category are, by design, rendered into policy documents published on Customer's Digital Properties.

Customer-configured forwarding

Where Customer configures a custom storage endpoint within the Services, Finsweet forwards a subset of each consent record to that Customer-controlled destination: the record identifier, the

action taken, the End User’s per-category choices, the literal banner text presented, the page URL, and the user agent string. Finsweet does not forward the pseudonymous user_identifier, the timestamp, the country-of-origin signal, or the specific trackers or providers associated with the choice. Customer, not Finsweet, controls that destination and determines what is done with the data once received there.

Sensitive data and special categories

The Services are not designed to process special categories of personal data within the meaning of Article 9 of the GDPR, and Customer shall not configure the Services so as to submit such data.

Customer acknowledges that consent purpose categories should not be configured in a manner that, by their labelling or granularity, reveals special category data about an End User.

For the purposes of US State Privacy Laws, Customer shall not submit sensitive personal information through the Services beyond that strictly necessary for their operation.

Frequency of transfer

Continuous, for the duration of the Agreement.

Duration and retention

Consent Data is retained in accordance with Section 4.3. Personal Data processed by Finsweet on Customer's behalf under this DPA, including Consent Data, is deleted or returned in accordance with Section 4.4 following termination. Company Account Data and Company Usage Data, which Finsweet processes as an independent controller under Section 12, are not within the scope of Section 4.4 and are instead retained as set out in Finsweet’s privacy policy.

Exhibit B — SCC Annex I and Annex III

1. The Parties

Data exporter:

Field	Information
Name	Customer, as identified in the Agreement
Address	As stated in the Agreement
Contact	As stated in the Agreement
Activities relevant to the transfer	Use of the Services, as described in Exhibit A
Role	Controller (or processor on behalf of a third-party controller)
Signature and date	Deemed executed on acceptance of this DPA

Data importer:

Field	Information
Name	Finsweet Inc.
Address	1732 Pettit Avenue, Unit A, Merrick, New York 11566, United States
Contact	privacy@finsweet.com
Activities relevant to the transfer	Provision of the Consent Pro service, as described in Exhibit A
Role	Processor (or sub-processor); controller in respect of Company Account Data and Company Usage Data
Signature and date	Deemed executed on acceptance of this DPA

2. Description of the transfer

All fields — categories of data subjects, categories of Personal Data, special category data, nature and purpose of processing, frequency, duration and retention — are as set out in **Exhibit A**.

3. Competent supervisory authority

The supervisory authority of the data exporter, determined in accordance with Clause 13 of the EU SCCs, including its rules for a data exporter not established in an EU Member State. For the purposes of the UK Addendum, the UK Information Commissioner's Office. For transfers subject to the Swiss FADP, the Swiss Federal Data Protection and Information Commissioner.

4. Annex III — Authorised Sub-Processors

Annex III for the purposes of the EU SCCs comprises only the recipients below, being those that process Personal Data within the Module Two/Three relationship this DPA documents — Consent Data, and other Personal Data Customer submits or instructs Finsweet to process in connection with the Services. It does not include vendors Finsweet engages in its own capacity as controller of Company Account Data and Company Usage Data (Section 12); those vendors are disclosed, together with every sub-processor Finsweet uses, on the current list referenced in Section 5.1, which is broader than this Annex by design.

Sub-processor	Purpose	Location	SCC Module
Cloudflare, Inc. (R2)	Consent record object storage.	Western Europe (WEUR)	Module 3 (P2P)

Cloudflare, Inc. (Workers, D1)	Edge delivery, CDN, security, and Consent Pro configuration/policy-generation content processed on Customer's instructions (excluding administrator account and identity data, which is Company Account Data under Section 12)	Global	Module 3 (P2P)
Cloudflare, Inc. (Browser Rendering)	Site scanning to detect cookies/trackers on Customer Digital Properties	Global	Module 3 (P2P)
Cloudflare, Inc. (Analytics Engine)	Aggregated consent statistics shown on Customer dashboards	Global	Module 3 (P2P)
Google LLC (Places API)	Address autocomplete in the policy-generation interface	Global	Module 3 (P2P)
OpenAI, L.L.C.	AI-assisted suggestions for tracker categorisation, purpose, retention and related configuration fields, and configuration form-fill assistance, using Customer-submitted tracker/provider configuration metadata. Certain free-text fields in this metadata are not filtered for Personal Data and could incidentally include it.	United States	Module 3 (P2P)

Note on SCC modules. Finsweet acts as a processor in respect of Consent Data. Transfers from Finsweet to a sub-processor of Consent Data, or of other Personal Data Customer submits or instructs Finsweet to process, are therefore processor-to-processor transfers requiring **Module 3**, not **Module 2** — all recipients currently listed in this Annex are Module 3 on that basis.

The current list of all of Finsweet's sub-processors — including those outside this Annex's SCC-specific scope, such as vendors Finsweet engages as controller of Company Account Data and Company Usage Data — is maintained at https://trust.finsweet.com/subprocessors, as referenced in Section 5.1.

Exhibit C — Technical and Organisational Measures (SCC Annex II)

Pseudonymisation and encryption. End User IP addresses are never persisted. On consent ingest, the IP address is combined with a secret value held by Finsweet, hashed using SHA-256, and truncated; only the resulting pseudonymous user_identifier is stored. The consent record identifier is supplied by the client and is not derived from the IP address. Regulatory jurisdiction is determined from country-level information provided at the network edge, and no finer-grained location is derived or retained.

Finsweet does not represent the user_identifier as anonymous data. Because Finsweet holds the secret value used in its derivation, the identifier remains pseudonymised Personal Data within the meaning of European Data Protection Laws and is protected as such under this DPA.

All data in transit and at rest is encrypted: Cloudflare encrypts stored objects, database files, snapshots and associated metadata with AES-256, with keys generated, stored and rotated within Cloudflare's production key management systems.

Confidentiality, integrity, availability and resilience. Customer agreements contain confidentiality obligations, and equivalent obligations are flowed down to Authorised Sub-Processors. Finsweet has completed a SOC 2 Type II audit covering the Security Trust Services Criterion.

Backup and recovery. Cloudflare D1 databases are automatically backed up by Cloudflare, supporting point-in-time restoration of the database as a whole to any point within the preceding 30 days; no backup is retained beyond that window.

Testing and evaluation. SOC 2 Type II audit covering the 2025 reporting period.

User identification and authorisation. Consent Pro administrators authenticate through one of two paths depending on how they access the Service: an administrator who onboards through the Consent Pro Webflow Designer Extension App authenticates using a Webflow ID token; an administrator using the Consent Pro Web App authenticates through Auth0, its default authentication method, which supports multi-factor authentication and single sign-on as optional, customer-enabled features — Finsweet does not enforce multi-factor authentication for administrator accounts. This is separate from Finsweet's own personnel access to production systems: under Finsweet's SOC 2 security protocols, Finsweet personnel are required to use two-factor authentication for production-system access, and this is enforced on each production system to the extent that system technically supports enforcement. Access is allocated by role on a least-privilege basis.

Protection during transmission. Secure methods and protocols are deployed for transmission of confidential information over public networks, using recommended cipher suites and TLS 1.2 or above.

Physical security. Finsweet does not operate or co-locate its own physical hardware. Physical security controls for the infrastructure and services used to process Personal Data are provided by the relevant third-party providers under their applicable security controls and certifications.

Event logging. Access to applications, tools and resources that process or store Personal Data is monitored. Records created and modified through the Consent Pro dashboard carry attribution metadata identifying the administrator responsible. Security logs are monitored by the security and engineering teams and escalated as appropriate.

System configuration. Changes to the production environment follow a documented change management process and are deployed through automated CI/CD tooling to ensure consistent configuration.

Certification and assurance. SOC 2 Type II audit covering the 2025 reporting period.

Data minimisation. The Services collect only the data necessary to record and evidence a consent choice and to determine the applicable regulatory framework. Raw IP addresses collected at End User consent ingest are discarded and never written to persistent storage. Location is resolved to country level only. Customer determines the consent purpose categories configured within the Services.

Data quality. Consent records are validated against a defined schema before persistence, using schema validation rules and strongly typed API contracts. Each record is bound to the template version presented at the time of capture, providing an auditable link between the consent given and the notice shown.

Limited retention. Consent Data is retained in accordance with Section 4.3. Personal Data processed by Finsweet on Customer's behalf is deleted or returned following termination in accordance with Section 4.4; Company Account Data and Company Usage Data are outside the scope of Section 4.4 and are retained as described in Exhibit A.

Accountability. Data protection and information security policies are maintained across the business, Personal Data Breaches are recorded and reported, and roles and responsibilities for information security and data privacy are formally assigned.

Portability and erasure. Customer may export Consent Data associated with an identified End User through the Services, and may access a specific record, including a Proof of Consent. Finsweet does not correct or edit a consent record once it has been recorded, and does not currently support self-service deletion of an individual End User's Consent Data through the Services. Finsweet shall action a Customer's access, export, or deletion request in accordance with Section 8.1.

Sub-processor measures. Finsweet subjects each Authorised Sub-Processor to binding contractual data-protection obligations as required by applicable Data Protection Law and, where applicable, the EU SCCs.

Exhibit D — UK Addendum

The International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the Information Commissioner's Office (Version B1.0), incorporated in full.

Part 1: Tables

Table 1: Parties

Attribute	Exporter (Customer)	Importer (Finsweet)
Start Date	This UK Addendum shall have the same effective date as the DPA.	Same as Exporter — this UK Addendum shall have the same effective date as the DPA.
Parties	Customer, as identified in Exhibit B, Section 1 (The Parties), which is incorporated into this Table by reference	Finsweet Inc., as identified in Exhibit B, Section 1 (The Parties), which is incorporated into this Table by reference
Key Contact	See Exhibit B	See Exhibit B

Table 2: Selected SCCs, Modules and Selected Clauses

Clause Item	Details
EU SCCs	The version of the Approved EU SCCs which this UK Addendum is appended to, as defined in the DPA and completed by Section 7.3 of the DPA.

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this UK Addendum is set out in:

Annex	Cross-Reference
Annex 1A: List of Parties	As per Table 1 above
Annex 1B: Description of Transfer	See Exhibit B
Annex II: Technical and organisational measures	See Exhibit C
Annex III: List of Sub-processors	See Exhibit B

Table 4: Ending this UK Addendum when the Approved UK Addendum Changes

Provision	Authorized Party
Ending this UK Addendum	Which Parties may end this UK Addendum as set out in Section 19: ☒ Importer ☐ Exporter ☐ Neither Party

Note: This provision permits the selected party (if any) to terminate the UK Addendum if the ICO changes the Approved UK Addendum which directly results in a substantial, disproportionate, and demonstrable increase in (a) its direct costs of performing its obligations under the UK Addendum or (b) its risk under the UK Addendum.

Part 2: Mandatory Clauses

The Parties adopt the Alternative Part 2 Mandatory Clauses mechanism the ICO makes available for this purpose, rather than reproducing the Mandatory Clauses in this DPA. Accordingly: 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, is incorporated by reference and forms part of this UK Addendum between the Parties.

End of DPA.