SMACKDAB INC. OFFICIAL POLICY

DATA PROCESSING ADDENDUM

Official legal PDF. This document is generated from the Smackdab website legal source file.

SMACKDAB INC. DATA PROCESSING ADDENDUM

Effective Date: April 26, 2025

Last Updated: September 9, 2026

Version:

2.3 – Free-account inactivity alignment

Document Location: https://smackdab.ai/legal/data-processing-addendum This Data Processing Addendum ("**DPA**") forms part of the Smackdab Inc. Terms of Service ("**TOS**" or "**Agreement**") available at https://smackdab.ai/legal/terms-of-service between Smackdab Inc. ("**Smackdab**") and the customer entity or individual ("**Client**" or "**Customer**") that has subscribed to the Services defined in the TOS. This DPA applies to the Processing of Personal Data (as defined below) contained within Client Data, where such Processing is subject to Applicable Data Protection Laws and where Smackdab acts as a Data Processor or Service Provider on behalf of the Client (acting as Data Controller or Business). This DPA prevails over any conflicting terms in the TOS regarding the Processing of Personal Data.

1. DEFINITIONS

Capitalized terms used but not defined in this DPA shall have the meanings given in the TOS or as defined below:

***1.1. "Applicable Data Protection Laws"** means all laws and regulations applicable to the Processing of Personal Data under the Agreement, including but not limited to the GDPR, UK GDPR, CCPA, CPRA, VCDPA (Virginia), CPA (Colorado), CTDPA (Connecticut), UCPA (Utah), and any related regulations.*

***1.2. "Client Data"** means the electronic data and information submitted by or for Client to the Services, as defined in the TOS, potentially containing Personal Data processed by Smackdab on behalf of Client. For clarity, references to "Client Data" in this DPA are equivalent to "Customer Data" as defined in the TOS. Personal Data refers to any information within Client Data that relates to an identified or identifiable natural person and is subject to Applicable Data Protection Laws.*

1.2a. "Data Retrieval Period" means the period following Account termination or expiration during which Client may retrieve its Personal Data from the Services before permanent deletion occurs. Unless otherwise specified in an applicable Order Form, the Data Retrieval Period is thirty (30) days from the date of termination or expiration.*

***1.3. "CCPA"** means the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 ("**CPRA**"), and any related regulations.*

***1.4. "Data Controller"** means the entity which determines the purposes and means of the Processing of Personal Data (typically the Client).*

***1.5. "Data Processor"** means the entity which Processes Personal Data on behalf of the Data Controller (typically Smackdab when Processing Client Data).*

***1.6. "Data Subject"** means the identified or identifiable natural person to whom Personal Data relates.*

***1.7. "EEA"** means the European Economic Area.*

***1.8. "GDPR"** means the General Data Protection Regulation (EU) 2016/679.*

***1.9. "Personal Data"** means any information relating to an identified or identifiable natural person contained within Client Data, processed by Smackdab on behalf of Client pursuant to the Agreement.*

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

***1.11. "Security Incident"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed by Smackdab as Data Processor.*

***1.12. "Service Provider"** has the meaning set forth in the CCPA.*

***1.13. "Standard Contractual Clauses"** or "**SCCs**" means the standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, as approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, currently available at https://eur-lex.europa.eu/eli/dec\impl/2021/914/oj. References to SCCs shall include the UK Addendum where applicable.*

1.14. "Sub-processor" *means any third-party Data Processor engaged by Smackdab to Process Personal Data contained in Client Data.*

1.15. "UK GDPR" *means the GDPR 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 2018 and amended by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (as amended).*

1.16. "UK Addendum" *means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner under S119A(1) Data Protection Act 2018, Version B1.0, in force 21 March 2022.*

---

2. ROLES AND SCOPE OF PROCESSING

2.1. Roles: *The parties acknowledge and agree that with regard to the Processing of Personal Data contained within Client Data, Client is the Data Controller (or a Processor acting on behalf of another Controller), and Smackdab is the Data Processor (or a Sub-processor acting on behalf of Client). Smackdab shall process Personal Data solely on behalf of the Client.*

2.2. Client Instructions: *Smackdab shall Process Personal Data only for the purposes described in this DPA and only in accordance with Client's documented lawful instructions, unless required to do otherwise by Applicable Data Protection Law to which Smackdab is subject. The Agreement (including this DPA and any applicable Order Forms) constitutes Client's complete and final instructions to Smackdab as of the Effective Date regarding the Processing of Personal Data. Any additional or alternate instructions must be agreed upon separately in writing via an amendment to this DPA. Client shall ensure its instructions for the Processing of Personal Data comply with Applicable Data Protection Laws. Client will have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Client acquired Personal Data.*

2.3. Processing Details: *The details of the Processing are as follows:*

- ***Subject Matter:*** *The subject matter of the Processing is the provision of the Services pursuant to the Agreement.*
- ***Duration:*** *The duration of the Processing is the term of the Agreement as specified therein, plus any post-termination period during which Smackdab may Process Personal Data as specified in Section 9 (Deletion or Return of Data).*
- ***Nature and Purpose:*** *The nature and purpose of the Processing is to provide the Services as initiated, configured, and used by the Client and its authorized Users. This includes storing, managing, retrieving, analyzing (as directed or configured by Client), communicating (as initiated by Client/Users), and otherwise processing Client Data as necessary to perform the Services, provide technical support, ensure security, prevent misuse, and comply with Client's instructions and the Agreement.*
- ***Categories of Data Subjects:*** *The categories of Data Subjects whose Personal Data is processed are determined and controlled by the Client in its sole discretion and may include, but are not limited to, Client's customers, potential customers (leads), employees, contractors, business partners, subscribers, website visitors, or other individuals interacting with the Client.*
- ***Types of Personal Data:*** *The types of Personal Data processed are determined and controlled by the Client in its sole discretion and may include, but are not limited to, names, contact details (email, phone, address), job titles, company information, communication content and logs, CRM records, marketing interaction data, financial information (if processed via Smackdab Pay subject to its agreement), user credentials (for authorized Users), or any other Personal Data Client chooses to upload, create, or manage within the Services. Client agrees not to store or process "Sensitive Data" (as defined in the TOS) or "Special Categories of Personal Data" (as defined by GDPR) within the standard fields of the Services, except where explicitly permitted by Smackdab for specific features designed for such data and subject to any additional required terms (e.g., an executed BAA for PHI).*

---

3. CLIENT OBLIGATIONS

3.1. Compliance: *Client represents and warrants that it shall comply with all Applicable Data Protection Laws regarding its collection and use of Personal Data and its use of the Services.*

3.2. Lawful Basis: *Client is solely responsible for ensuring it has established and will maintain a valid lawful basis (e.g., consent, contract necessity, legitimate interest) for the Processing of all Personal Data submitted to the Services by Client or its Users.*

3.3. Notices and Consents: *Client is responsible for providing all necessary privacy notices to Data Subjects and obtaining all necessary rights, permissions, and consents required by Applicable Data Protection Laws for Smackdab to lawfully Process the Personal Data on Client's behalf for the purposes contemplated by the Agreement.*

---

4. SMACKDAB OBLIGATIONS AS DATA PROCESSOR

4.1. Processing According to Instructions: *Smackdab shall Process Personal Data only in accordance with Client's documented instructions as set forth in Section 2.2. Smackdab shall immediately inform Client if, in Smackdab's opinion, an instruction infringes Applicable Data Protection Laws (provided that this does not require Smackdab to provide legal advice).*

4.2. Confidentiality: *Smackdab shall ensure that its personnel authorized to Process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.*

4.3. Security: *Smackdab shall implement and maintain appropriate technical and organizational security measures designed to protect the security, confidentiality, and integrity of Personal Data Processed on behalf of the Client against Security Incidents. These measures shall be appropriate to the risk, considering the state of the art, costs of implementation, and the nature, scope, context, and purposes of Processing. Such measures are further described in https://smackdab.ai/legal/security-policy.*

4.4. Sub-processing:

- *Client grants Smackdab general written authorization to engage Sub-processors to assist in providing the Services, subject to the terms herein.*
- *Smackdab shall maintain a current list of its Sub-processors at https://smackdab.ai/legal/sub-processors (**"Sub-processor List"**).*
- *Smackdab shall provide Client with prior notice (e.g., via email or account notification) of any intended changes concerning the addition or replacement of Sub-processors. Client may object in writing to the appointment of a new Sub-processor within thirty (30) days of such notice, provided that the objection is based on reasonable data protection grounds. If Client objects, Smackdab will use reasonable efforts to make available a change in the Services or recommend a commercially reasonable change to Client's configuration or use of the Services to avoid Processing by the objected-to Sub-processor. If Smackdab is unable to make available such change within a reasonable period, either party may terminate the applicable Order Form(s) with respect only to those Services which cannot be provided by Smackdab without the use of the objected-to Sub-processor by providing written notice to the other party.*
- *Smackdab shall enter into a written agreement with each Sub-processor imposing data protection obligations substantially similar to those set out in this DPA.*
- *Smackdab shall remain fully liable to the Client for the performance of that Sub-processor's data protection obligations.*

4.5. Data Subject Rights Assistance: *Taking into account the nature of the Processing, Smackdab shall provide reasonable assistance to the Client, upon Client's written request and at Client's expense, by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Client's obligation to respond to requests from Data Subjects exercising their rights under Applicable Data Protection Laws. Smackdab shall promptly notify Client if it receives a request directly from a Data Subject related to their Personal Data processed under this DPA, unless prohibited by law. Client is responsible for validating and responding to such requests.*

4.6. Assistance with Compliance: *Taking into account the nature of Processing and the information available to Smackdab, Smackdab shall provide reasonable assistance to Client, at Client's expense, in ensuring compliance with Client's obligations pursuant to Articles 32 to 36 of the GDPR (Security, Breach Notification, DPIAs) or similar obligations under other Applicable Data Protection Laws.*

4.7. Audits: *Upon Client's reasonable written request (no more than once annually, unless required by law or following a Security Incident), Smackdab shall make available to Client information reasonably necessary to demonstrate compliance with this DPA. Smackdab shall allow for and contribute to audits, including inspections, conducted by the Client or an independent third-party auditor mandated by the Client (subject to confidentiality obligations and not being a competitor), at Client's sole expense. The scope, timing, and duration shall be agreed upon in advance to minimize disruption. Smackdab may satisfy this requirement by providing relevant current third-party audit reports (e.g., SOC 2 Type II) or certifications upon request.*

---

5. SECURITY INCIDENT NOTIFICATION

5.1. Smackdab's Notification to Client (Processor Obligation): *If Smackdab becomes aware of a confirmed Security Incident affecting Personal Data Processed under this DPA, Smackdab shall notify Client without undue delay and in any event within forty-eight (48) hours of becoming aware of the Security Incident. The notification will, where feasible:*

5.2. Content of Notification.** The notification to Client will, where feasible, include: *(a) describe the nature of the Security Incident; (b) describe the likely consequences and categories of Personal Data and Data Subjects affected; (c) describe the measures taken or proposed to be taken by Smackdab to address the Security Incident and mitigate its effects; (d) provide the name and contact details of Smackdab's Data Protection Officer or security contact; and (e) provide other reasonably available information Client may need to meet its own notification obligations under Applicable Data Protection Laws*

5.3. Client's Notification Responsibilities (Controller Obligations). *Smackdab's notification to Client within 48 hours initiates the incident response process. Client, as the Data Controller (or as a Processor acting on behalf of a Controller), is solely responsible for determining whether and how to notify:*

(i) Supervisory Authorities: Client must notify the competent supervisory authority (e.g., relevant Data Protection Authority) within seventy-two (72) hours of becoming aware of the confirmed Security Incident, as required by Article 33 of the GDPR or equivalent provisions under other Applicable Data Protection Laws. This is Client's independent legal obligation, separate from and in addition to Smackdab's 48-hour notification to Client. **(ii) Affected Data Subjects**: Client must notify affected individuals of the Security Incident without undue delay, in accordance with applicable law and regulatory guidance, including GDPR Article 34 or equivalent provisions. Notification requirements and timelines vary by jurisdiction and the severity of the breach.* **(iii) Other Authorities:** Client must comply with any other applicable legal requirements regarding notification to law enforcement, regulators, or other third parties (e.g., Florida's 30-day requirement for residents under Fla. Stat. § 501.171).**

5.4. Smackdab Cooperation. *Smackdab will provide reasonable assistance to Client in meeting Client's notification obligations, including providing additional information about the Security Incident, guidance on risk assessment, and cooperation with regulatory investigations, as reasonably requested by Client. Smackdab will also, where permissible and in consultation with Client, cooperate with law enforcement and regulatory authorities.**

5.5. No Admission of Liability. *Smackdab's notification of a Security Incident shall not be construed as an admission of fault, liability, or breach of any obligation under this DPA or applicable law.**

5.6. Vendor/Sub-processor Notification Upstream.*Smackdab's ability to meet this 48-hour notification commitment depends on timely notification from its own vendors and sub-processors. All vendor and sub-processor agreements contain breach notification requirements requiring notification to Smackdab immediately and, in any event, no later than 24 hours of discovery. This 24-hour upstream requirement ensures Smackdab has sufficient time to triage, analyze, and fulfill its 48-hour notification obligation to Client. For details on Smackdab's vendor management practices and breach notification protocols, see the Security Policy at https://smackdab.ai/legal/security-policy.*

5.7. Clarification Table. | *Party* | *Responsibility* | *Timeline* | *Legal Basis* |

|-------|----------------|----------|------------|

| Smackdab|Notify Client of confirmed Security Incident|48 hours of becoming aware|DPA 5.1 (Processor obligation) |

| Client | Notify Supervisory Authority | 72 hours from discovery | GDPR Art. 33 (Controller obligation) |

| Client | Notify Affected Individuals | As required by law (varies) | GDPR Art. 34, state privacy laws |

| Smackdab | Cooperate with Client & authorities | Reasonable efforts | DPA § 5.4 |

---

6. INTERNATIONAL TRANSFERS

6.1. Processing Locations: *Client acknowledges Smackdab primarily Processes Personal Data in the United States. Sub-processors may be located in the U.S. or other countries as per the Sub-processor List.*

6.2. Transfer Mechanism: *If the Processing of Personal Data under this DPA involves a transfer subject to GDPR or UK GDPR data transfer restrictions to a country not recognized as providing an adequate level of protection (e.g., from EEA/UK/Switzerland to the U.S.), the parties agree that the Standard Contractual Clauses (SCCs) are incorporated by reference and apply as follows:*

- ***Module Applicability:*** *Module Two (Controller to Processor) applies where Client is a Controller. Module Three (Processor to Processor) applies where Client is a Processor acting on behalf of another Controller.*
- ***Clause Specifics:*** *Clause 7 (Docking Clause) does not apply. Clause 9(a) Option 2 (General written authorization for sub-processors) applies, with the notice period specified in Section 4.4 above. Clause 11(a) (Redress) optional language does not apply. For Clauses 17 and 18, the governing law and jurisdiction shall be those specified in the main Agreement (TOS), unless required otherwise by Applicable Data Protection Law (e.g., law of EU Member State for Clause 17, Irish law/courts for Clause 18(c) where no EU Member State law applies).*
- ***Annexes:*** *The information required by Annex I and II of the SCCs is contained within this DPA (esp. Section 2.3), the Agreement, the Sub-processor List, and Smackdab's security documentation referenced herein or provided separately. Annex III (List of Sub-processors) is the Sub-processor List referenced in Section 4.4.*
- ***UK Addendum:*** *For transfers subject to the UK GDPR, the SCCs apply as amended by the UK Addendum, with Part 1 of the UK Addendum populated as follows: Parties details from the Agreement, Key Contact details from the Agreement/account info, Annex 1 A/B and Annex II details from this DPA/Agreement/Security Docs, Annex III details from Sub-processor List. Option for Importer to notify ICO under Table 4 is not selected.*
- ***Swiss Transfers:*** *_For transfers of data subject to the Swiss Federal Data Protection Act, the SCCs will also apply with the following adaptations:*

(i) references to the GDPR are to be understood as references to the Swiss Federal Data Protection Act;

(ii) references to the EU or Member State are to be understood as references to Switzerland; and

(iii) references to the competent supervisory authority and competent courts are replaced with the Swiss Federal Data Protection and Information Commissioner and competent Swiss courts._

- ***Conflict:*** *In case of conflict between this DPA and the SCCs/UK Addendum, the SCCs/UK Addendum shall prevail.*

---

7. CCPA SERVICE PROVIDER TERMS

Where applicable, Smackdab maintains certification under the EU–US Data Privacy Framework (DPF) as an additional safeguard; however, the SCCs (with UK Addendum/Swiss adaptations) remain the primary transfer mechanism

7.1. Role: *Smackdab acts as a Service Provider for Personal Information Processed under this DPA on behalf of Client, when Client is subject to the CCPA.*

7.2. Obligations: *Smackdab certifies it understands the restrictions under CCPA §1798.140(ag) and agrees it will not:*

(a) "sell" or "share" Personal Information; (b) retain, use, or disclose Personal Information for any purpose other than the specific business purposes outlined in Section 2.3 of this DPA and performed on behalf of Client, or as otherwise permitted by CCPA; (c) retain, use, or disclose Personal Information outside the direct business relationship between Smackdab and Client, unless permitted by CCPA; (d) combine Personal Information received from Client with Personal Information from other sources, except as necessary to perform the Services or as permitted by CCPA.

Smackdab will comply with applicable obligations under the CCPA and provide the same level of privacy protection as required of businesses. Smackdab will notify Client if it determines it can no longer meet its CCPA obligations.

7.3. Client Rights: *Client has the right to take reasonable steps to ensure Smackdab uses Personal Information consistent with Client's CCPA obligations and to stop and remediate unauthorized use.*

---

8. DATA RETENTION

Smackdab retains Client Data processed within the Service according to the instructions of the applicable Client, or for the duration specified in our agreement with the Client. Upon termination of the Client's account or specific instruction from the Client, Smackdab will delete Client Data in accordance with the terms of the TOS and DPA, as described in Section 9 of this DPA, unless retention is required by law

Termination of an eligible ongoing free account for inactivity under TOS Section 3.4 is a termination for purposes of this Section and Section 9. That rule applies only when incorporated into the applicable Agreement in accordance with its amendment or acceptance requirements. It does not authorize earlier deletion, remove the Data Retrieval Period, or override Client instructions or retention obligations under this DPA. Individual integration disconnection alone does not terminate the account or begin the deletion period.

---

9. DELETION OR RETURN OF PERSONAL DATA

Following inactivity termination, Smackdab will maintain a secure means for the Client or an authorized representative to retrieve or export Personal Data throughout the 30-day Data Retrieval Period, without requiring restoration of ordinary account use.

Upon termination or expiration of the Agreement, or upon Client's written request, Smackdab shall securely delete Personal Data in accordance with the following timeline: Production systems: Personal Data shall be deleted from active production systems within thirty (30) days after expiration of the Data Retrieval Period.*

Backup systems: Data in backup systems shall be overwritten or destroyed no later than ninety (90) days after deletion from production systems.

Total retention period: The maximum total retention period, including both production and backup systems, shall not exceed one hundred eighty (180) days from the end of the Data Retrieval Period.

These timelines control notwithstanding any contrary language in other documents.

For Beta or preview Services: *Personal Data may be deleted* ***at any time without notice,*** *and the Data Retrieval Period and deletion timeline above* ***do not apply****.*

The Client is solely responsible for backing up and exporting any Personal Data before the Beta Period ends or before Smackdab discontinues the Beta Services.

Upon Client's request, Smackdab will provide written certification of the deletion of Personal Data within thirty (30) days of completion of the deletion process.

10. GENERAL

10.1. Conflict—Data Protection Super-Precedence. *Notwithstanding any other provision in the TOS, Order Form, Beta/Early Access Terms, API Terms of Use, Product-Specific Terms, or any other agreement or policy, this DPA shall* ***always and exclusively prevail*** *with respect to:*

- *Personal Data processing, retention, deletion, and handling; - Compliance with Applicable Data Protection Laws (GDPR, UK GDPR, CCPA, VCDPA, CPA, CTDPA, UCPA, etc.); - Data security, encryption, and access controls; - Breach notification and incident response for Personal Data; - Sub-processor management and vendor compliance related to Personal Data; - Data subject rights (access, correction, deletion, portability); - Data protection impact assessments and compliance documentation; - Any other matter relating to the privacy, security, or protection of Personal Data.*

This super-precedence applies regardless of whether the Personal Data is processed through Beta Services, API endpoints, Product-Specific features, or any other Smackdab offering.

Where this DPA conflicts with any other document on any data protection matter, this DPA controls exclusively for that data protection aspect, while the other document may continue to control non-data-protection aspects of the same service.

For all other matters not related to data protection and Personal Data processing (e.g., billing disputes, API usage limits, Beta feature limitations, service warranties, or disputes between other policies), the document hierarchy set forth in TOS Section 15.7 shall apply.

***Example**: If Beta Terms and this DPA both address "Beta data upon service termination," the DPA shall control deletion timelines and Personal Data handling (Section 9), while Beta Terms may control other Beta access and use limitations.*

***10.2. Governing Law:** This DPA and any disputes arising out of it shall be governed by the law specified in the Governing Law section of the TOS, unless otherwise required by Applicable Data Protection Law or the SCCs.*

***10.3. Amendments:** This DPA may only be amended by a written agreement signed by authorized representatives of both parties, except that Smackdab may unilaterally update this DPA as necessary to comply with Applicable Data Protection Laws or the SCCs, providing notice to Client of material changes. Updates under this Section will not materially reduce the protections for Personal Data during Customer's active term.*

***10.4. Severability:** If any provision of this DPA is found invalid or unenforceable, the remainder shall continue in full force and effect.*

***10.5. Notice**: All notices related to this DPA shall be sent to the following addresses: To Smackdab: Smackdab Inc. Attn: Data Protection Officer 372 Live Oak Ln Marco Island, FL 34145 Email: privacy@smackdab.ai **To Client** The address and contact information provided in the applicable Order Form or as updated by Client in its account settings. IN WITNESS WHEREOF, the parties agree this DPA is effective as of the date the Client accepted the TOS or executed an Order Form incorporating this DPA by reference. (Note: Electronic acceptance of TOS typically includes acceptance of the DPA). --- *© 2025 Smackdab Inc. All rights reserved.**

This PDF is the formal downloadable version of DATA PROCESSING ADDENDUM.