SMACKDAB INC. OFFICIAL POLICY

PRIVACY POLICY

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

SMACKDAB INC. PRIVACY POLICY

Effective Date: April 26, 2025

Last Updated: September 9, 2026

Version: 3.4 – Free-account inactivity alignment

EXECUTIVE SUMMARY

Smackdab Inc. ("**Smackdab**," "**we**," "**us**," or "**our**") is committed to protecting your privacy. This Privacy Policy explains how we collect, use, disclose, and safeguard your personal data when you use our services (the "**Subscription Service**" or "**Service**"), visit our websites (including **smackdab.ai** and related sites), or otherwise interact with us.

Key Points:

- We act as a **Controller** when you provide personal data directly to us (e.g., when creating an account)
- We act as a **Processor** (or "service provider") when our customers use our Service to process their end users' data
- We implement robust security measures to protect your data
- You have specific rights regarding your personal data, which vary by jurisdiction
- We may transfer data internationally with appropriate safeguards in place
- We use cookies and similar technologies subject to your consent where required
- We use privacy-protective session replay and interaction analytics on our websites to understand usage, troubleshoot issues, and improve the user experience
- We do not sell or share your personal data for monetary or other valuable consideration as defined under applicable privacy laws
- We maintain Records of Processing Activities in compliance with GDPR Article 30

- In the event of a Security Incident affecting Customer Data, we will notify the Customer within 48 hours of becoming aware. The Customer notifies individuals and authorities. For a breach of data we control (our website, marketing, and billing contacts), we will notify affected individuals and authorities as required by law, including Florida's 30-day rule.
- We conduct regular privacy training for all employees with access to personal data

For detailed information, please read the full policy below. If you have questions, please contact us at privacy@smackdab.ai or our Data Protection Officer at dpo@smackdab.ai.

---

1. DATA CONTROLLER VS. PROCESSOR ROLES

Smackdab acts in different roles depending on the context in which personal data is processed:

1.1. Controller Role: Smackdab acts as a **data controller** (or "**business**" under U.S. state privacy laws) when you provide personal data directly to us – for example, by creating an account, subscribing to our Service, visiting our websites, contacting sales or support, or attending a Smackdab event or webinar. In these cases, we determine the purposes and means of processing your personal data. We use this information to provide and administer our services, communicate with you, improve and promote our offerings, and for other legitimate business purposes as described in this Policy.

1.2. Processor Role: Smackdab acts as a **data processor** (or "**service provider**" under U.S. state privacy laws) on behalf of our customers when they use our Service to store, manage, or process personal data about their contacts, leads, or end users in connection with their own business activities (for example, managing customer relationships or sending proposals to their clients). In this context, the customer is the data controller and Smackdab processes such **Customer Data** only on the customer's instructions and in accordance with our Data Processing Addendum ("**DPA**") and Customer Terms of Service. Our customers are responsible for providing any necessary notices and obtaining any required consents from individuals before submitting their personal data to the Service. For purposes of this Privacy Policy, "**Personal Data**" (or "**personal information**") means any information that relates to an identified or identifiable individual. This may include, but is not limited to, name, email address, postal address, phone number, and online identifiers.

---

2. WHAT INFORMATION WE COLLECT AND PROCESS

We collect various types of information from and about you depending on how you interact with us and our Service:

<hr />

2.1 Information You Provide to Smackdab

We collect Personal Data that you voluntarily provide to us when interacting with Smackdab websites or using our Service:

2.1.1 Website Visitors and Contact Requests

- Name, work email address, phone number
- Job title, company name, industry
- Mailing address or other contact details
- Information provided in forms (demo requests, content downloads, support inquiries)
- Marketing preferences and communication history

2.2.2 Account Registration and User Information

- Name, email address, username, password
- Contact details and profile information
- Company information and business details
- User roles and permissions
- Authentication credentials

2.2.3 Payment and Billing Information

- Billing name and address
- Payment method details (e.g., last four digits of credit card, payment card type)
- Financial account information (handled securely by our payment processors)
- Billing history and subscription details
- Tax information where required

2.1.4. Communications and Support

- Email correspondence and support-chat transcripts between you and Smackdab (not in-product Customer Data such as SmackChat messages)
- Support tickets and issue descriptions
- Call recordings obtained with your consent through:

(i) notification at the beginning of calls that the call may be recorded and your continued participation,

(ii) or express verbal or written agreement. For EU/UK/Swiss customers, we obtain explicit consent in accordance with applicable data protection laws. We record calls for quality assurance, training, dispute resolution, and regulatory compliance. You may decline recording by ending the call.

- Feedback and survey responses

- Testimonials and reviews (with your explicit consent for public use)
- Communication metadata including timestamps and interaction history

<hr />

2.2 Information We Process on Behalf of Customers

Our Service enables our customers to input, store, and manage Personal Data about their own contacts and end users as part of using the CRM and proposal software. This data may include:

- Contact information (name, email, phone, address)
- Professional information (job title, company, department)
- Communications and interaction history
- Transaction records and purchase history
- Document content (proposals, contracts, attachments)
- Any other information customers choose to include

We refer to this as "**Customer Data**." Smackdab processes Customer Data on behalf of the customer according to their instructions. We generally have no direct relationship with the individuals whose Personal Data is contained in Customer Data. The customer is responsible for ensuring lawful collection and processing, providing appropriate notices, and handling data subject requests.

<hr />

2.3 Information We Collect When You Use the Service

When you interact with the Smackdab Service, we automatically collect certain information:

2.3.1 Usage Data

- Features and modules accessed
- Pages or screens visited
- Time, date, and duration of interactions
- Actions taken (e.g., creating proposals, updating records)
- Frequency and patterns of use
- Performance metrics and analytics

2.3.2 Device and Log Data

- Internet Protocol (IP) address
- Browser type, version, and language
- Device type, operating system, and device identifiers

- Screen resolution and settings
- Geographic location (country, region, city)
- Internet service provider
- Entry/exit pages and referral URLs
- Search terms used to reach our site
- Error logs and crash reports

2.3.3 Website Interaction and Session Replay Data

When you visit our public websites, we may use session replay and interaction analytics technologies to understand how visitors use our pages. These tools may collect:

- Pages visited, clicks, taps, scrolling, navigation paths, page timing, and other interaction events
- Session identifiers, visitor identifiers, entry pages, device type, browser information, and user agent information
- Visual replay data showing how a visitor interacted with the website

We use this information for troubleshooting, debugging, improving website usability, measuring engagement, and understanding which pages or features are useful to visitors.

We do not use session replay to collect personal information that you type into website forms. Text entry fields, including text, email, telephone, number, and password fields, are masked before replay data is collected. This means the replay may show that a visitor interacted with a form field, but it is designed not to capture the personal typed content entered into that field.

2.3.4 Mobile Application Data (if applicable)

- Mobile device identifiers
- Device model and manufacturer
- Operating system type and version
- App version and update information
- Mobile network information
- Device permissions and settings

2.3.5 Third-Party Integration Data

- Information from connected third-party services (with your authorization)
- API access and usage statistics
- Connection status and syncing information
- Authentication tokens (securely stored)

- Integration configuration settings

<hr />

2.4 Information We Collect from Other Sources

We may obtain information about you from other sources to supplement the information you provide:

2.4.1 Partners and Resellers

- Contact information from referral partners
- Business details from authorized resellers
- Account information from implementation partners
- Integration data from technology partners

2.4.2 Public Sources

- Professional information from company websites
- Business contact details from professional directories
- Public profiles on LinkedIn or similar platforms
- Industry information and affiliations
- Public company information

2.4..3 Third-Party Services

- Updated contact information from data providers
- Market research and business intelligence
- Advertising and marketing analytics
- Event registration information

Account activity records. We record authenticated interactive sign-in/use timestamps, user identity, and the account in which activity occurs to administer the separate integration and account inactivity rules in TOS Section 3.4. Automated syncing and session maintenance do not count as human activity for that policy.

---

3. HOW WE USE PERSONAL DATA

We use the Personal Data we collect for the following purposes:

3.1 To Provide and Manage the Service

- Create and maintain your account

- Authenticate users and secure access
- Provide the features and functions you request
- Process payments and manage subscriptions
- Provide customer support and troubleshooting
- Facilitate communication between users
- Maintain service records and documentation

We also use these activity records to identify eligible inactive free users or accounts, send service notices, cancel pending actions when users return, and administer disconnection, deactivation, and post-termination export and deletion under the Agreement.

3.2 To Improve and Develop Our Products

- Analyze usage patterns and feature adoption
- Identify and resolve technical issues
- Develop new features and enhancements
- Conduct research and product development
- Test and optimize performance
- Review masked session replay and interaction analytics to debug website issues and improve usability
- Gather feedback and measure satisfaction

3.3 To Communicate With You

- Send service-related notices and updates
- Provide essential account information
- Respond to your inquiries and requests
- Deliver support and technical assistance
- Send confirmation emails and notifications
- Share product tips and best practices

3.4 For Marketing and Promotional Purposes (with your consent where required)

- Send newsletters and content updates
- Provide information about products and features
- Invite you to events and webinars
- Deliver promotional offers and incentives
- Conduct surveys and gather feedback

- Create custom audiences for advertising

3.5 To Maintain Security and Prevent Fraud

- Verify identity and authenticate access
- Monitor for suspicious or unauthorized activity
- Detect and prevent security breaches
- Protect against fraud and abuse
- Enforce our Terms of Service and policies
- Maintain audit logs and security records

3.6 To Comply With Legal Obligations

- Meet regulatory requirements
- Respond to legal requests and proceedings
- Establish, exercise, or defend legal claims
- Maintain required business records
- Conduct audits and investigations
- Enforce our agreements and policies

3.7 Artificial Intelligence and Machine Learning Smackdab may use artificial intelligence (AI) and machine learning (ML) technologies in certain aspects of our Service:

- **How We Use AI/ML:** We may use AI/ML to enhance features like search functionality, content recommendations, data analytics, and predictive capabilities within the Service.
- **Types of Data Used:** These systems are trained and operated using:
- Anonymized and aggregated usage patterns
- Non-personal technical data
- User interactions with features (with consent where required)
- In some cases, Customer Data when explicitly configured by the Customer
- **Opt-Out Rights:** Where AI/ML features process your Personal Data for purposes beyond basic service provision:
- You will receive clear notice before such processing occurs
- You can opt out via your account settings or by contacting us

- Opting out will not affect core functionality of the Service
- **Algorithmic Decision-Making:** We do not make fully automated decisions with legal or similarly significant effects without human oversight.

Any automated decision-making is subject to appropriate safeguards, including human review, testing for bias, explanation of logic used, and the right to contest the outcome.

- **Model Ownership:** Any AI models developed using our data are owned by Smackdab. This ownership does not affect your Personal Data rights, which remain fully protected under applicable privacy laws. Any Personal Data used in model training will be processed in accordance with our Data Processing Agreement and applicable privacy regulations.

3.8 Legal Basis for Processing (EEA, UK, and similar jurisdictions) If you are located in the European Economic Area (EEA), United Kingdom, or another jurisdiction that requires a legal basis for processing personal data, we rely on the following grounds:

- **Performance of a Contract:** Processing necessary to provide the Service according to our agreement with you
- **Legitimate Interests:** Processing that serves our legitimate business interests (such as security, fraud prevention, and service improvement) without unduly impacting your rights
- **Consent:** Processing based on your specific permission (such as for certain marketing activities)
- **Legal Obligation:** Processing required to comply with our legal obligations

When we rely on legitimate interests, we balance our interests against potential impacts on your privacy and conduct formal Legitimate Interest Assessments where required by law. If we process data based on consent, you can withdraw that consent at any time.

---

4. HOW WE SHARE PERSONAL DATA

We do not sell your Personal Data to third parties for monetary consideration. However, we may share your Personal Data in the following circumstances:

4.1 Service Providers We share data with trusted third-party service providers who perform services on our behalf, such as:

- Cloud hosting and infrastructure providers
- Payment processors and billing services
- Email delivery and communication platforms
- Customer support and help desk tools
- Analytics and performance monitoring

- Marketing automation platforms
- Security and fraud prevention services

These providers are contractually obligated to use Personal Data only for the purposes of providing services to us and to maintain appropriate security measures.

4.2 Business Partners We may share limited information with our business partners:

- Referral partners (when you came through their referral)
- Resellers or channel partners that support your account
- Integration partners when you enable their services
- Implementation consultants with your permission
- Co-marketing partners (with your consent)

Partner sharing is limited to what is necessary for the specific business relationship.

4.3 With Your Consent We may share Personal Data with third parties when you explicitly consent to such sharing, such as:

- When you choose to enable third-party integrations
- When you participate in testimonials or case studies
- When you elect to share information publicly
- When you direct us to share your information

4.4 Corporate Transactions If Smackdab is involved in a merger, acquisition, financing, reorganization, bankruptcy, or sale of company assets, your information may be transferred as part of that transaction. We will notify you of any such change in ownership or control of your Personal Data through our website or by direct communication.

4.5 Legal Requirements We may disclose your information if required to do so by law or in response to valid requests by public authorities (e.g., court order, government request). We may also disclose information if we believe in good faith that disclosure is necessary to:

- Comply with legal obligations
- Protect and defend our rights or property
- Prevent or investigate possible wrongdoing
- Protect the personal safety of users or the public
- Protect against legal liability

4.6 Aggregated or De-identified Data We may share aggregated or de-identified information, which cannot reasonably be used to identify you, with third parties for research, marketing, analytics and other purposes,

provided such information does not identify you.

---

5. HOW WE TRANSFER PERSONAL DATA INTERNATIONALLY

Smackdab is headquartered in the United States, but we serve customers around the world. Your Personal Data may be transferred to, stored in, and processed in countries other than your own.

5.1 Transfer Mechanisms When we transfer Personal Data from the European Economic Area (EEA), United Kingdom, Switzerland, or other regions with data protection laws to countries not deemed to provide adequate protection, we implement appropriate safeguards including:

- **Standard Contractual Clauses (SCCs):** We use the European Commission's approved Standard Contractual Clauses in our agreements with service providers and affiliates.
- **UK International Data Transfer Agreement (IDTA):** For transfers involving UK data, we implement the UK IDTA or the UK Addendum to the EU SCCs.
- **Swiss Transborder Data Flow Agreement:** For transfers involving Swiss data, we use appropriate Swiss transfer mechanisms.
- **Supplementary Measures:** Following the Schrems II decision, we implement additional technical, organizational, and contractual measures to enhance protection for transferred data, including:
- End-to-end encryption where technically feasible
- Pseudonymization of certain data elements
- Robust access controls and authentication
- Transparency regarding government access requests
- Contractual commitments regarding government data requests
- Data minimization practices for international transfers

5.2 Transfer Impact Assessments We conduct and regularly update data transfer impact assessments (TIAs) for countries where data is processed, considering:

- The nature of the Personal Data being transferred
- The relevant laws of the destination country
- The practical application and enforcement of those laws
- The technical and organizational measures implemented
- The risk of government access to the data

- The availability of effective remedies for data subjects

These assessments are reviewed at least annually or whenever there are significant changes to privacy regulations, data protection laws, or court decisions affecting international data transfers. The assessments inform our approach to implementing supplementary measures where necessary.

5.3 Data Subject Remedies for International Transfers Individuals whose Personal Data is transferred internationally have the following rights and remedies:

- The right to lodge a complaint with a supervisory authority in the EEA, UK, or Switzerland
- The right to judicial remedies in courts with jurisdiction over Smackdab or the relevant data exporter
- The right to receive compensation for damages resulting from violations of the transfer safeguards
- The ability to enforce third-party beneficiary rights under the SCCs or other transfer mechanisms
- Access to the competent courts as specified in the applicable SCCs or transfer agreements

5.4 Data Localization (where applicable) For customers with specific data localization requirements, we may offer regional data storage options as specified in your service agreement. Our current data storage options include:

- United States (primary)
- European Union (upon request with additional fees)
- United Kingdom (upon request with additional fees)

Please contact us for more information about available data residency options and associated costs.

---

6. HOW WE STORE AND SECURE PERSONAL DATA

6.1 Data Security Smackdab implements and maintains appropriate technical and organizational security measures designed to protect your Personal Data from unauthorized access, disclosure, alteration, or destruction. These measures include:

- Encryption of data in transit using TLS 1.2+ protocols
- Encryption of sensitive data at rest using AES-256 encryption
- Network security controls including firewalls and intrusion detection
- Multi-factor authentication for administrative access
- Regular security assessments and penetration testing
- Access controls based on the principle of least privilege
- Regular security awareness training for personnel
- Physical security measures for our facilities and equipment

- System monitoring and logging of access and activities
- Incident response procedures and recovery capabilities
- Privacy by design in system development
- Regular backups with secure storage
- Vendor security assessments for third-party providers

All Smackdab employees undergo mandatory privacy and security training upon hiring and at least annually thereafter. This training covers data protection laws, secure handling of personal data, recognizing and reporting security incidents, and our internal privacy policies and procedures. While we implement industry-standard safeguards and regularly update our security measures, no security system is impenetrable. We implement reasonable technical and organizational measures to protect your data, but the transmission of information via the internet carries inherent risks. Any transmission is at your own risk, though we maintain cyber liability insurance and incident response procedures to address potential security incidents.

6.2 Data Retention We retain Personal Data for as long as necessary to provide the services you have requested, comply with our legal obligations, resolve disputes, and enforce our agreements:

- **Account Data:** We keep your account information for as long as your account is active, plus a defined period after account closure to comply with legal requirements and handle any post-termination matters.
- **Customer Data:** We retain Customer Data according to our agreement with the customer and delete or return it as specified in our DPA and Terms of Service.
- **Marketing Data:** We retain marketing information until you opt-out or request deletion, after which we may maintain minimal records to honor your preferences.
- **Usage Data:** We retain usage data for a limited period (typically 12-24 months) to support security, troubleshooting, and service improvement.
- **Session Replay Data:** We retain website session replay data for a limited period (typically 30 days) to support troubleshooting, debugging, usability improvement, and analytics.
- **Legal Requirements:** We may retain certain data for longer periods if required by law, for tax purposes, accounting, or to comply with other legal obligations.

For ongoing free accounts, TOS Section 3.4 distinguishes individual integration inactivity from account inactivity. Paid accounts are exempt. Account deactivation for inactivity starts the existing 30-day Data Retrieval Period; it does not immediately erase data. Customer Data then follows the production and backup deletion schedule below and in DPA Section 9. Disconnecting an individual integration does not itself trigger that deletion schedule.

Specific retention periods for different data categories are listed in the table below:

Data Category

Typical Retention Period

Retention Basis

Account Information

Duration of account + 7 years for contract, billing-contact, and invoice-level records required by law. Profile fields that are not required for tax or contract are deleted under the Customer Data lifecycle below.

Legal obligation, contract performance

Payment Records

Duration of account + 7 years

Tax and accounting requirements

Customer Data

Life of the Customer account, unless the Customer sets a shorter period. After termination: 30-day Data Retrieval Period, then production deletion within 30 days, backups within 90 days of production deletion, total ≤ 180 days from the end of the Data Retrieval Period (DPA §9). Includes in-product chat messages and attachments.

Customer instruction, contract terms

Usage Logs

12-24 months

Security, service improvement

Marketing Data

Until opt-out + 3 years

Legitimate interest, consent

Communication Records

Duration of relationship + 2 years. Means Smackdab support tickets and our correspondence with you only. Does not include Customer Data or in-product chat.

Support, legal protection

Website Logs

90 days

Security, performance analysis

Website Session Replay Data

30 days

Troubleshooting, debugging, usability improvement, analytics

Biometric Data (if any)

Duration of specific purpose + 3 years

Explicit consent, specific purpose

When Personal Data is no longer needed, we will securely delete or anonymize it in accordance with our data retention policies, unless retention is required by applicable law or legitimate business purposes.

6.3 Data Breach Notification In the event of a confirmed breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data, we will:

- **When we are the processor (Customer Data, including in-product chat):** We will notify the Customer without undue delay and within 48 hours of becoming aware of a confirmed Security Incident. The Customer is solely responsible for notifying individuals, supervisory authorities, and other third parties, including the GDPR 72-hour authority notice and Florida's 30-day individual notice where they apply.
- **When we are the controller (our website, marketing, account, and billing data):** We will notify affected individuals and relevant supervisory authorities as required by law, including without undue delay and, where feasible, within 72 hours of becoming aware if the incident is likely to result in a risk to individuals. For Florida residents, no later than 30 days after determination of a breach (Fla. Stat. § 501.171).
- **Notification Content:** Our notification will include at minimum:
- The nature of the breach
- Categories and approximate number of individuals affected
- Categories and approximate number of data records concerned
- Name and contact details of our Data Protection Officer or other contact point
- Description of likely consequences of the breach
- Description of measures taken or proposed to address the breach
- Recommendations for affected individuals to mitigate potential adverse effects
- **Ongoing Assessment:** We maintain an internal breach response team that assesses the severity of any data incident according to a formal risk assessment methodology.
- **Documentation:** We document all breaches of Personal Data, including the facts relating to the breach, its effects, and the remedial action taken, regardless of whether notification was required.
- **Post-Incident Review:** Following any data security incident, we conduct a thorough review to identify root causes and implement preventative measures.

7. COOKIES AND SIMILAR TECHNOLOGIES

7.1 Cookies and Tracking Technologies Smackdab uses cookies and similar tracking technologies (such as web beacons, pixels, local storage, device identifiers, session replay, and interaction analytics technologies) to automatically collect certain information when you visit our websites or use our Service. Details about these technologies, how we use them, and your choices regarding them are available in our separate https://smackdab.ai/legal/cookie-policy

7.2 Types of Cookies We Use We classify cookies into the following categories:

- **Strictly Necessary Cookies:** Essential for the basic functionality of our websites and services
- **Functional Cookies:** Remember your preferences and settings to enhance your experience
- **Performance/Analytics Cookies:** Help us understand how visitors interact with our site
- **Session Replay and Interaction Analytics:** Help us review masked website interaction data, such as clicks, scrolling, navigation paths, and page timing, so we can troubleshoot issues and improve the site
- **Targeting/Advertising Cookies:** Used to deliver relevant ads and track campaign effectiveness

7.3 Your Cookie Choices You have the right to decide whether to accept or reject cookies (except Strictly Necessary cookies). You can exercise your cookie preferences through:

- Your browser settings (to control cookies at the browser level)
- Industry opt-out pages for interest-based advertising

For complete information about our use of cookies and your choices, please see our Cookie Policy.

7.4 Third-Party Identifiers In addition to cookies, various third parties may place and read identifiers on your device for advertising, analytics, and functionality purposes:

- **Advertising IDs:** Mobile devices use advertising identifiers (Apple's IDFA, Google's Advertising ID) that allow apps and advertisers to track user activity for advertising purposes while providing user control.
- **Pixel Tags:** Transparent images embedded in web pages or emails that collect information about your device, browsing activity, and email engagement. We use pixels from services like Google Analytics, Facebook, and LinkedIn.
- **Local Storage:** HTML5 local storage allows websites to store larger amounts of data on your device than cookies.

We use local storage for improving site performance and user experience.

- **Device Fingerprinting:** Your device's unique combination of settings, installed fonts, plugins, and other technical characteristics can create a "fingerprint" that might be used for identification across websites.

- **Cross-Site Tracking:** Some third parties may attempt to recognize you across different websites or services using various identifiers or combinations of identifiers.

For each type of identifier, you have specific opt-out options:

- For mobile advertising IDs, use your device privacy settings (iOS: Settings > Privacy > Tracking; Android: Settings > Privacy > Ads)
- For third-party pixel tracking, use browser privacy settings and ad blockers
- For local storage, clear your browser's cache and local storage
- For device fingerprinting, consider using privacy-focused browsers and extensions

We honor Global Privacy Control (GPC) signals from browsers and extensions that support this feature.

---

8. YOUR PRIVACY RIGHTS AND CHOICES

Depending on your country or region, you may have certain rights regarding your Personal Data. We honor all applicable data protection rights afforded to individuals under relevant laws.

8.1 Access and Portability You have the right to request:

- Confirmation of whether we process your Personal Data
- Access to your Personal Data
- Information about how we process your data
- A copy of your Personal Data in a structured, commonly used, and machine-readable format

For data portability requests, we will provide your data in a standard format (such as CSV, JSON, or XML) that can be imported into other systems.

8.2 Correction and Updating You have the right to request correction of inaccurate Personal Data or completion of incomplete data. You can update certain information directly through your account settings or by contacting us.

8.3 Deletion and Restriction You have the right to request:

- Deletion of your Personal Data (subject to certain exceptions)
- Restriction of processing while we verify or investigate your concerns
- Withdrawal of your consent, where processing is based on consent

8.4 Objection and Automated Decisions You have the right to:

- Object to processing based on legitimate interests
- Object to direct marketing at any time

- Not be subject to decisions based solely on automated processing that produce legal effects, unless necessary for a contract or you've given explicit consent

8.5 How to Exercise Your Rights To exercise any of these rights, please:

- Email us at privacy@smackdab.ai
- Write to us at the address in the Contact Us section (Section 16)
- Use the specific rights management tools in your account

We will respond to legitimate requests as soon as practicable and in accordance with applicable law (typically within 30-45 days). We may request specific information to verify your identity before fulfilling your request. In some cases, we may have legal grounds to deny or limit the scope of your request, in which case we will explain our reasoning.

8.6 Unsubscribing from Communications You can unsubscribe from our marketing communications at any time by:

- Clicking the "unsubscribe" link in any marketing email
- Adjusting your communication preferences in your account
- Contacting us at privacy@smackdab.ai

Even if you opt out of marketing, you will still receive transactional communications related to your account and the Service.

8.7 Do Not Track Some browsers have "Do Not Track" (DNT) features. Because there is not yet a common understanding of how to interpret DNT signals, we do not currently respond to them. You can use other tools described in this policy to control data collection and use.

---

9. STATE-SPECIFIC PRIVACY RIGHTS

9.1 California Privacy Rights If you are a California resident, the California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA), provides you with specific rights:

- **Right to Know:** You can request disclosure of categories and specific pieces of Personal Information we have collected, the sources of collection, business purposes, and categories of third parties with whom we share the information.
- **Right to Delete:** You can request deletion of your Personal Information, subject to certain exceptions.
- **Right to Correct:** You can request correction of inaccurate Personal Information.
- **Right to Opt-Out of Sale/Sharing:** While we do not sell Personal Information for monetary consideration, some of our advertising and analytics activities might be considered "sharing" under the CPRA. You can opt out of this sharing for cross-context behavioral advertising as described in Section

8.5. If you opt out, there is the possibility that you will also no longer be eligible to use one or more of our Services.

- **Right to Limit Use of Sensitive Personal Information:** You can direct us to limit the use of sensitive personal information to what is necessary for the service.
- **Right to Non-Discrimination:** We will not discriminate against you for exercising your CCPA rights.

For information on categories of Personal Information we collect and disclose, see Sections 2 and 4. To exercise your rights, see Section 8.5 or email privacy@smackdab.ai with "California Privacy Rights" in the subject line.

9.2 Virginia, Colorado, Connecticut, and Utah Residents Residents of Virginia (VCDPA), Colorado (CPA), Connecticut (CTDPA), and Utah (UCPA) have similar rights regarding:

- Confirmation and access
- Correction
- Deletion
- Data portability
- Opting out of targeted advertising, sales, and profiling
- Non-discrimination

Each state has specific requirements and timelines for responding to requests. Please contact us at privacy@smackdab.ai to exercise your rights under these laws.

9.3 Nevada Residents Nevada residents have the right to opt out of the sale of their Personal Information. However, we do not sell Personal Information as defined under Nevada law (NRS 603A). If you have questions, please contact privacy@smackdab.ai.

9.4 Biometric Information Privacy Certain jurisdictions have enacted specific laws governing the collection, use, storage, and disposal of biometric information, including the Illinois Biometric Information Privacy Act (BIPA), Texas Biometric Privacy Law, and Washington's biometric privacy provisions.

9.4.1 Our Collection and Use of Biometric Information Smackdab may potentially collect or process biometric information in limited circumstances:

- **Voice Recordings:** If you use our communication features or call recordings, we may process voice data. While we generally do not use voice recognition for identification purposes, certain advanced features might analyze vocal patterns.
- **Facial Recognition:** We do not use facial recognition technology in our standard Services. If facial recognition becomes available in future features, it will be strictly opt-in.
- **Other Biometric Data:** Will destroy biometric information when the initial purpose for collecting it has been satisfied, or within 3 years of the individual's last interaction with us, whichever occurs first, unless a longer retention period is required by law or ongoing litigation

9.4.2 Notice and Consent Before collecting or processing any biometric information, we will:

- Provide clear, specific written notice explaining:
- That biometric information is being collected or stored
- The specific purpose and length of time for which the information will be collected, stored, and used
- Obtain a written release or express consent from the affected individual

9.4.3 Data Security and Retention For any biometric information we collect, we:

- Protect it using the same security standards we apply to other sensitive Personal Data
- Store, transmit, and protect it using reasonable security measures that are the same as or exceed industry standards
- Will destroy biometric information when the initial purpose for collecting it has been satisfied, or within 3 years of the individual's last interaction with us, whichever occurs first

9.4.4 No Sale or Profit We will not sell, lease, trade, or otherwise profit from an individual's biometric information.

9.4.5 Customer Obligations If you are a customer using our Services to collect or process biometric information of your own end users, you are responsible for complying with all applicable biometric privacy laws, including providing appropriate notices, obtaining consent, and implementing required security measures.

---

10. CHILDREN'S PRIVACY

10.1 Age Restrictions Smackdab's websites and services are not intended for, nor directed to, children under the age of 13. We do not knowingly collect personal information from children under 13 years old. If we learn we have collected Personal Data from a child under 13 without verified parental consent, we will promptly delete that information. If you believe we might have any information from or about a child under 13, please contact us at privacy@smackdab.ai.

10.2 Children's Data in the Subscription Service Our customers might use Smackdab to manage information about their own clients or contacts, which could potentially include individuals under the age of 16. In such cases:

- The customer is responsible for ensuring they have obtained appropriate parental consent
- The customer must comply with all applicable child privacy laws (such as COPPA)
- Such data is handled solely as Customer Data according to our agreements
- We recommend customers not include children's personal information unless absolutely necessary

11. THIRD-PARTY WEBSITES AND SERVICES

Our websites and communications may contain links to third-party websites, plug-ins, or services that are not owned or controlled by Smackdab. When you click on those links, you may be sending information to a third party whose privacy practices we do not control. This Privacy Policy does not cover the information practices of third-party websites or services linked to or integrated with our Service. We encourage you to review the privacy policies of any third-party site you visit or service you use. We are not responsible for the privacy practices or content of such third parties.

12. GOOGLE PRODUCT INTEGRATIONS

Smackdab offers certain integrations with Google products to enhance the functionality of our Service. If you choose to use these integrations, you will be asked to grant Smackdab access to specific data from your Google account.

12.1 Google reCAPTCHA We use Google reCAPTCHA to prevent spam and abuse. This service collects hardware and software information and sends it to Google for analysis. Google's use of this information is governed by Google's Privacy Policy.

12.2 Gmail Integration If you integrate Gmail with Smackdab, we may access content from your emails (with your consent) to provide features like email tracking or inbox management. We do not use this data for advertising or to build profiles beyond your use of our Service.

12.3 Google Calendar Integration With Google Calendar integration, we may access calendar data to display availability or associate meetings with CRM contacts. We only use this information to provide the integration functionality you request.

12.4 Google Drive Integration If you connect Google Drive, we will request permission to view and manage files you specifically choose to use with Smackdab. We will only access files you select or create through our interface.

12.5 Compliance with Google API Services User Data Policy Our use of information received from Google APIs adheres to Google's API Services User Data Policy, including the Limited Use requirements. We only use such data to provide or improve features you explicitly request, and we do not use this data for advertising or other unrelated purposes. Furthermore, we explicitly affirm that any data received from Google APIs, including data accessed through Gmail and Google Calendar integrations (e.g., email content, calendar data), is used solely to provide or improve user-facing features within the Smackdab Service and is *not* used to develop, improve, or train generalized artificial intelligence (AI) and/or machine learning (ML) models.

13. CHANGES TO THIS PRIVACY POLICY

We may update this Privacy Policy from time to time to reflect changes in our practices, technologies, legal requirements, or other factors. If we make material changes, we will notify you by:

- Posting the updated policy on our website with an updated "Last Updated" date
- Sending an email to the primary email address associated with your account
- Displaying a notice through the Service interface

For material changes to how we handle Personal Data, we will provide at least thirty (30) days' advance notice before the changes take effect, as required by TOS §15.16(a), unless a shorter period is required by law or for urgent security reasons. Your continued use of the Service after the effective date of any changes constitutes your acceptance of the revised Privacy Policy. If you do not agree with the changes, you should discontinue your use of the Service and contact us to close your account. We maintain an archive of previous versions of this Privacy Policy, which may be requested by contacting privacy@smackdab.ai. We encourage you to review this Privacy Policy periodically to stay informed about our privacy practices.

14. ACCESSIBILITY

14.1 Accessible Format We are committed to ensuring that our Privacy Policy and privacy-related communications are accessible to all individuals, including those with disabilities. This Privacy Policy is designed to be compatible with screen readers and other assistive technologies.

14.2 Alternative Formats Upon request, we will provide this Privacy Policy and privacy-related communications in alternative formats, such as:

- Large print
- Braille
- Audio recording
- HTML or other machine-readable formats
- Simplified language versions

14.3 Accessibility Assistance If you need assistance accessing or understanding our Privacy Policy or exercising your privacy rights due to a disability, we can provide:

- Direct telephone support
- Guided assistance through forms and procedures
- Extended time if needed to complete any verification processes
- Alternative methods for identity verification if standard methods are not accessible

14.4 Web Content Accessibility Guidelines Our digital privacy communications, including this Privacy Policy, are designed to conform with Web Content Accessibility Guidelines (WCAG) 2.1 Level AA standards. To request accessibility assistance, please contact accessibility@smackdab.ai or call +1 (239) 299-4616.

---

15. DATA PROTECTION GOVERNANCE

15.1 Data Protection Officer Smackdab has appointed a Data Protection Officer (DPO) responsible for overseeing our privacy program and ensuring compliance with data protection laws. Our DPO's duties include:

- Monitoring compliance with data protection laws and our internal policies
- Advising on data protection impact assessments
- Cooperating with data protection authorities
- Serving as a contact point for data subjects and supervisory authorities
- Leading our privacy by design initiatives

You may contact our DPO directly at dpo@smackdab.ai.

15.2 Records of Processing Activities In compliance with Article 30 of the GDPR, we maintain comprehensive records of our personal data processing activities. These records document:

- The purposes of processing
- Categories of data subjects and personal data
- Categories of recipients
- International transfers and safeguards
- Retention schedules
- Technical and organizational security measures

These records are maintained in electronic format and are made available to supervisory authorities upon request.

15.3 Data Protection Impact Assessments We conduct Data Protection Impact Assessments (DPIAs) before implementing new technologies or processing activities that may pose high risks to individuals' privacy. Our DPIA process:

- Identifies and assesses privacy risks
- Implements measures to mitigate identified risks
- Documents compliance considerations
- Involves consultation with relevant stakeholders

15.4 Privacy by Design and Default We implement privacy by design and default principles in our system development processes by:

- Considering privacy implications from the earliest stages of product development
- Building privacy controls directly into our systems and processes
- Setting privacy-protective default settings
- Minimizing data collection to what is necessary
- Implementing privacy-enhancing technologies

---

16. CONTACT US

If you have any questions, concerns, or requests regarding this Privacy Policy or our privacy practices, please contact us: **Email:** privacy@smackdab.ai **Mail:** Smackdab Inc. Attn: Privacy Team 372 Live Oak Ln Marco Island, FL 34145 United States **Phone:** +1 (239) 299-4616 **Data Protection Officer:** dpo@smackdab.ai If you need this Privacy Policy in an alternative format due to a disability, please contact us and we will work with you to provide the information in a format that is accessible to you. **© 2025 Smackdab Inc. All rights reserved.**

This PDF is the formal downloadable version of PRIVACY POLICY.