Privacy Policy

Effective Date: April 5, 2026

1. Introduction

FlockFactor LLC, doing business as Primavay (“Primavay,” “we,” “us,” or “our”), respects your privacy and is committed to protecting the personal information you share with us. This Privacy Policy explains what data we collect, how we use it, how we protect it, and your rights regarding that data.

We will never sell, rent, or trade your personal information to third parties. Period.

This policy applies to all users of our website (primavay.com), client portal, intake form, and related services, regardless of location. By using our services, you acknowledge that you have read and understood this Privacy Policy.

2. Information We Collect

Account Information: When you create an account, we collect your email address and a password (which is securely hashed and stored by our authentication provider, Supabase). We never have access to your plaintext password.

Intake Form Data: When you submit your intake form, we collect the information you provide: your name, email, phone number, venue name, venue details, style preferences, special requests, and any photographs or logo files you upload.

Payment Information: Payment processing is handled entirely by Stripe. We do not store credit card numbers, bank account details, or other sensitive financial information on our servers. Stripe may share limited information with us (such as the last four digits of your card, your email, billing address, and transaction amounts) for order management purposes.

Usage Data: We collect basic server logs and request metadata (such as IP addresses, browser type, referring URL, and timestamps) for security, rate limiting, and abuse prevention. We do not use tracking cookies or third-party analytics services.

Communications: If you contact us via email, we retain the content of your messages and our responses for customer service and record-keeping purposes.

Information We Do NOT Collect: We do not collect biometric data (including facial recognition data from photographs you upload — photos are used solely for website design and are not processed through any facial recognition or biometric analysis system). We do not collect precise geolocation data. We do not collect financial account numbers or social security numbers. We do not collect data from third-party sources about you.

3. Legal Basis for Processing (GDPR)

If you are located in the European Economic Area (EEA), United Kingdom, or Switzerland, we process your personal data on the following legal bases:

Contractual Necessity (Article 6(1)(b)): Processing your account data, intake form data, and payment data is necessary to perform our contract with you (delivering your website and managing your subscription).

Legitimate Interest (Article 6(1)(f)): Processing server logs and usage data for security, abuse prevention, and platform integrity is based on our legitimate interest in maintaining a safe and functional service. We have conducted a balancing test and concluded that these interests do not override your fundamental rights.

Legal Obligation (Article 6(1)(c)): We may retain certain data (such as transaction records) where required by tax, accounting, or other legal requirements.

Consent (Article 6(1)(a)): Where we process data based on your consent, you may withdraw that consent at any time by contacting us at hello@primavay.com. Withdrawal does not affect the lawfulness of processing performed prior to withdrawal.

4. How We Use Your Information

We use the information we collect solely for the purpose of delivering and improving our services:

To deliver your website: Your intake form data, photos, and preferences are used by our design team to build your custom website.

To communicate with you: We send transactional emails related to your project (status updates, preview notifications, delivery confirmations, payment receipts, and revision confirmations). These emails are sent from hello@primavay.com via our email delivery provider, Resend.

To manage your account: Your email address is used for authentication, account verification, and to link your portal account to your project.

To process payments: Your payment information is processed by Stripe. We use Stripe-provided transaction data to track subscription status and billing history.

To protect our platform: IP addresses and request data are used for rate limiting and preventing abuse. This data is processed in memory and is not stored long-term.

To improve our services: We may use aggregated, de-identified data to analyze service usage patterns and improve our platform. This data cannot be used to identify any individual user.

5. Automated Decision-Making & Profiling

We do not engage in automated decision-making or profiling that produces legal effects or similarly significant effects on you. No decisions about your service, pricing, eligibility, or account status are made solely by automated means. All significant decisions are made by human team members.

6. Data Storage & Security

Your data is stored using industry-standard, trusted infrastructure providers:

Database & Authentication: Supabase (managed PostgreSQL, hosted on AWS). Your account data, project data, intake submissions, and activity logs are stored in Supabase's cloud infrastructure. Supabase encrypts data at rest (AES-256) and in transit (TLS 1.2+). Passwords are securely hashed using bcrypt and are never stored in plaintext.

File Storage: Photos and deliverable files are stored in Supabase Storage with row-level access controls. Download links are time-limited (1-hour expiry) and require authentication and project ownership verification.

Payments: All payment data is processed and stored by Stripe, which is PCI-DSS Level 1 certified (the highest level of payment security certification).

Email: Transactional emails are sent through Resend. Your email address is shared with Resend solely for the purpose of delivering emails related to your project.

Hosting: Our application is hosted on Vercel, which provides SSL/TLS encryption for all connections and operates on edge infrastructure with DDoS protection.

Security Measures: In addition to our providers' security, we implement: role-based access controls limiting data access to authorized personnel; input validation and sanitization to prevent injection attacks; rate limiting on all API endpoints; time-limited, authenticated download links for file access; and regular security reviews of our codebase.

While we implement commercially reasonable security measures, no method of transmission over the internet or method of electronic storage is 100% secure. We cannot guarantee absolute security of your data.

7. Data Sharing & Sub-Processors

We do not sell, rent, or trade your personal information. We have never sold personal information and have no plans to do so.

We share data only with the following service providers (sub-processors) and only to the extent necessary to deliver our services:

Supabase Inc. — Database, authentication, and file storage (USA). Processes: account data, project data, intake submissions, uploaded files.

Stripe, Inc. — Payment processing (USA, PCI-DSS Level 1). Processes: payment method data, transaction data, billing information.

Resend, Inc. — Email delivery (USA). Processes: email addresses, email content for transactional messages.

Vercel Inc. — Application hosting (USA, global edge). Processes: IP addresses, request metadata for serving the application.

Each of these providers maintains their own privacy policies, security certifications, and data processing agreements. We do not share your data with advertisers, data brokers, social media companies, or any other third parties for marketing, profiling, or advertising purposes.

We may disclose information if required by law, such as in response to a valid subpoena, court order, or government request, or if disclosure is reasonably necessary to protect our rights, your safety, or the safety of others, prevent fraud, or comply with a judicial proceeding.

8. International Data Transfers

Our services and infrastructure providers are based in the United States. If you are accessing our services from outside the United States (including from the European Economic Area, United Kingdom, Switzerland, Canada, or other regions with data protection laws), your data will be transferred to, stored, and processed in the United States, which may not offer the same level of data protection as your home country.

Transfer Safeguards: We rely on the standard contractual clauses (SCCs) approved by the European Commission and the UK International Data Transfer Agreement (IDTA), as well as the data processing agreements maintained by our infrastructure providers, to provide appropriate safeguards for international data transfers. You may request a copy of the relevant transfer mechanisms by contacting us at hello@primavay.com.

By using our services, you acknowledge and consent to the transfer and processing of your information in the United States as described in this policy.

9. Your Rights

Depending on your location, you may have some or all of the following rights regarding your personal data:

Access: You can view your project data, intake details, and revision history through your client portal at any time. You may also request a complete copy of all personal data we hold about you.

Download: Your website files are always available for download from your portal. They are yours to keep.

Deletion: You may request deletion of your account and associated personal data by emailing us at hello@primavay.com. We will process deletion requests within 30 days (or within the timeframe required by your jurisdiction's applicable law, if shorter). We may retain certain data as required by law or for legitimate business purposes (such as transaction records for tax compliance).

Correction: If any of your information is inaccurate, contact us and we will correct it promptly.

Data Portability: You may request your personal data in a structured, commonly used, machine-readable format (such as JSON or CSV).

Restriction of Processing: You may request that we restrict processing of your personal data in certain circumstances, such as while we verify the accuracy of data you have disputed.

Objection: Where we process data based on legitimate interest, you have the right to object. We will cease processing unless we demonstrate compelling legitimate grounds that override your interests.

Withdrawal of Consent: Where processing is based on consent, you may withdraw that consent at any time without affecting the lawfulness of processing performed prior to withdrawal.

Opt-out of Communications: Transactional emails (project updates, payment notifications) are essential to service delivery and cannot be opted out of while you have an active project or subscription. If you have no active project or subscription, you will not receive any emails from us. We do not send marketing or promotional emails.

To exercise any of these rights, contact us at hello@primavay.com. We will respond within 30 days (or sooner if required by applicable law). We will verify your identity before processing data access or deletion requests. **We will not discriminate against you for exercising any of your privacy rights.**

10. California Privacy Rights (CCPA/CPRA)

If you are a California resident, you have rights under the California Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act (CPRA):

Right to Know: You have the right to request that we disclose the categories and specific pieces of personal information we have collected about you, the categories of sources from which it was

collected, the business or commercial purpose for collecting it, and the categories of third parties with whom we share it.

Right to Delete: You have the right to request deletion of your personal information, subject to certain exceptions permitted by law (such as completing a transaction, detecting security incidents, or complying with legal obligations).

Right to Correct: You have the right to request that we correct inaccurate personal information.

Right to Opt-Out of Sale or Sharing: We do not sell or "share" (as defined by the CCPA/CPRA) your personal information to third parties for cross-context behavioral advertising. We have not sold or shared personal information in the preceding 12 months and have no plans to do so.

Right to Limit Use of Sensitive Personal Information: We do not use or disclose "sensitive personal information" (as defined by the CPRA) for purposes beyond those necessary to provide our services.

Right to Non-Discrimination: We will not discriminate against you for exercising any of your CCPA/CPRA rights, including by denying services, charging different prices, or providing a different level of quality.

Categories of Data Collected: In the preceding 12 months, we have collected the following categories of personal information: identifiers (name, email, phone number, IP address); commercial information (purchase history, subscription status); internet or other electronic network activity information (server logs, portal usage); and professional or employment-related information (venue/business details). We collect this data directly from you and from Stripe (limited transaction data).

Retention: We retain each category of data as described in Section 13 (Data Retention).

Authorized Agent: You may designate an authorized agent to submit requests on your behalf. We will require verification of the agent's authority and your identity.

To submit a verifiable consumer request, contact us at hello@primavay.com. We will verify your identity before processing your request and respond within 45 days as required by law.

11. Additional U.S. State Privacy Rights

If you are a resident of Virginia, Colorado, Connecticut, Utah, Oregon, Texas, Montana, Indiana, Kentucky, Rhode Island, or another state with a comprehensive consumer privacy law, you may have additional rights, including the right to access, correct, delete, and obtain a copy of your personal data, and the right to opt out of the sale of personal data, targeted advertising, and certain profiling.

We do not sell personal data, engage in targeted advertising, or profile consumers for decisions that produce legal or similarly significant effects. Therefore, many of these opt-out rights are already satisfied by our practices.

Right to Appeal: If we decline your privacy request, you have the right to appeal our decision. To appeal, email us at hello@primavay.com with “Privacy Appeal” in the subject line. We will respond to your appeal within the timeframe required by your state’s applicable law. If your appeal is denied, you may contact your state’s Attorney General to submit a complaint.

Ohio Residents: While Ohio does not currently have a comprehensive state consumer privacy law, Ohio residents are protected by the Ohio Consumer Sales Practices Act (ORC § 1345.01 et seq.) and Ohio’s data breach notification law (ORC § 1349.19). If you have concerns about how your data is handled, you may file a complaint with the Ohio Attorney General’s Consumer Protection Section at (800) 282-0515 or online at www.ohioprotects.org.

12. EEA, UK & Swiss Residents (GDPR)

If you are located in the European Economic Area, United Kingdom, or Switzerland, you have additional rights under the General Data Protection Regulation (GDPR) or equivalent legislation:

Data Controller: FlockFactor LLC (d/b/a Primavay) is the data controller for the personal data we process. Contact: hello@primavay.com.

Your Additional Rights: In addition to the rights listed in Section 9, you have the right to lodge a complaint with your local data protection supervisory authority if you believe our processing of your personal data violates applicable law. A list of EEA supervisory authorities is available at the European Data Protection Board website.

Data Protection Officer: Due to the nature and scale of our operations, we have not appointed a formal Data Protection Officer. For all privacy inquiries, contact us at hello@primavay.com.

Data Processing Agreements: If you require a Data Processing Agreement (DPA) as a data controller engaging our services, please contact us at hello@primavay.com and we will provide one.

See Section 3 for the legal bases on which we process your data, Section 5 for automated decision-making disclosures, and Section 8 for information on international data transfers.

13. Cookies & Tracking

Essential Cookies Only: We use essential (strictly necessary) cookies solely for authentication — maintaining your login session. These cookies are required for the basic functionality of our platform and do not require separate consent under the GDPR’s ePrivacy Directive, as they fall within the “strictly necessary” exemption.

We do not use: advertising or marketing cookies; analytics cookies (Google Analytics, Mixpanel, etc.); social media tracking pixels (Facebook Pixel, etc.); third-party tracking scripts of any kind; cross-site tracking; or fingerprinting technologies.

Do Not Track Signals: Some browsers transmit “Do Not Track” (DNT) signals. Because we do not engage in any tracking beyond essential authentication cookies, our practices are consistent with DNT signals regardless of whether one is received. We honor all “Do Not Track,” “Global Privacy Control” (GPC), and similar opt-out preference signals.

14. Data Retention

We retain your data only as long as necessary for the purposes described in this policy:

Account data: Retained for the lifetime of your account. Deleted within 30 days of account closure.

Intake form data & project data: Retained for the lifetime of your account. Deleted within 30 days of account closure.

Uploaded photos & files: Retained for the lifetime of your account. Removed from storage within 30 days of account closure.

Deliverable files: Available for download for the lifetime of your account. Removed within 30 days of account closure (ensure you download your files before closing your account).

Payment transaction records: Retained for up to 7 years after the transaction date, as required by U.S. tax and accounting regulations (IRS record-keeping requirements).

Server logs & security data: Retained for no more than 90 days, then automatically purged.

Email communications: Retained for up to 3 years after the last interaction for customer service and dispute resolution purposes.

Upon account deletion, we will remove or de-identify all personal data within 30 days, except for records we are legally required to retain as specified above.

15. Data Breach Notification

In the event of a data breach that compromises the security or confidentiality of your personal information, we will notify affected users in the most expedient time possible and without unreasonable delay, and in no event later than 72 hours after becoming aware of the breach.

Ohio Residents (ORC § 1349.19): If you are an Ohio resident and we experience a breach of the security of the system involving your personal information (as defined by Ohio Revised Code § 1349.19 — your name in combination with unencrypted Social Security number, driver’s license number, or financial account numbers with access codes), we will notify you in the most expedient time possible and without unreasonable delay as required by Ohio law. If the breach affects more than 1,000 Ohio residents, we will also notify all nationwide consumer reporting agencies. Note: We do not collect Social Security numbers, driver’s license numbers, or financial account numbers — these are processed

exclusively by Stripe. However, we include this disclosure for full transparency regarding our obligations.

All Users: Breach notifications will include: the nature of the breach; the types of data affected; the likely consequences; the measures we are taking to address and mitigate the breach; and steps you can take to protect yourself. Where required by law, we will also notify relevant supervisory authorities (for GDPR), state Attorneys General, and/or consumer reporting agencies within the required timeframes.

We maintain an internal incident response plan and conduct periodic reviews of our security practices.

16. Children's Privacy

Our services are designed for businesses (event venues) and are not directed to individuals under the age of 18. We do not knowingly collect personal information from children under the age of 13 (or under 16 in the EEA/UK). We do not have actual knowledge that we sell or share personal information of consumers under the age of 16.

If you believe we have inadvertently collected data from a child under 13 (or the applicable age in your jurisdiction), please contact us immediately at hello@primavay.com. We will promptly verify and delete the data within 48 hours of confirmation.

In compliance with the Children's Online Privacy Protection Act (COPPA) and the FTC's amended COPPA Rule (effective April 22, 2026), we do not knowingly collect, use, or disclose personal information from children under 13 without verifiable parental consent.

17. Third-Party Links & Services

Our website, portal, and emails may contain links to third-party websites or services (such as Stripe's billing portal). We are not responsible for the privacy practices, security, or content of those third-party sites. This Privacy Policy does not apply to any third-party services, and we encourage you to review the privacy policies of any third-party services you access. We are not liable for any damages arising from your use of third-party services linked from our platform.

18. Changes to This Policy

We may update this Privacy Policy from time to time. If we make material changes, we will notify you via email at least thirty (30) days before the changes take effect. The effective date at the top of this page indicates when the policy was last revised. We will maintain an archive of prior versions of this policy, available upon request. Your continued use of our services after the effective date constitutes acceptance of the updated policy. If you do not agree with the changes, you may close your account

before the effective date.

19. Contact & Complaints

If you have questions about this Privacy Policy, wish to exercise any of your data rights, or have concerns about how your data is handled, please contact us at:

FlockFactor LLC (d/b/a Primavay)

Email: hello@primavay.com

We aim to respond to all inquiries within 30 days. If you are not satisfied with our response, you may lodge a complaint with your local data protection authority (for EEA/UK/Swiss residents) or your state's Attorney General (for U.S. residents).