MPC Privacy Policy

MPC Solutions, LLC is committed to protecting the privacy of the organizations and individuals who use the MPC Solutions Platform. This Privacy Policy explains what information we collect, how we use it, and your rights.

This Policy applies to: (1) Client organizations using the Platform; (2) individual Users within those organizations; and (3) individuals whose data is stored by Clients, such as donors, board members, volunteers, and participants ("End Subjects").

1. Information We Collect

1.1 Account and Registration Information

Organization name, EIN (optional), website, contact information, billing address, and administrator name and email. For individual users: name, email address, job title, and platform role.

1.2 Authentication Information

We offer sign-in via email/password and Google SSO. When you use Google SSO, we receive your name, email, and profile photo from Google. We do not store your Google password. Authentication is managed by Supabase Auth (SOC 2 Type 2 certified).

1.3 Client Data You Input

As you use the Platform, you may store information about third parties, including:

- Donor and constituent records (names, contact information, giving history, communication preferences)
- Grant and funder information (funder details, application data, award records)
- Board member information (names, contact details, terms, COI disclosures)
- Volunteer records (names, contact information, skills, background check status, hours)
- Program participant data (demographics, enrollment status, service records)
- Financial records (budget data, expense records, fund information)

You are responsible for ensuring you have the appropriate legal basis to collect and store this information.

1.4 Usage and Technical Data

We automatically collect IP address, browser type, operating system, pages visited, features used, and timestamps to improve the Platform and for security monitoring.

1.5 Payment Information

Payment processing is handled by Stripe, Inc. We do not store full card numbers or CVV. We retain only a tokenized reference and basic billing information as provided by Stripe.

1.6 Communications

If you contact us, we retain those communications to respond to inquiries and improve our services.

2. How We Use Your Information

We use collected information to:

- Provide, maintain, and improve the Platform
- Authenticate users and manage account access
- Process payments and send billing communications
- Send transactional emails such as deadline reminders, security notifications, and acknowledgment templates

- Send product updates and feature announcements (you may opt out at any time)
- Respond to support requests
- Monitor security, detect fraud, and enforce our Terms of Service
- Analyze aggregate usage patterns and improve the Platform experience
- Comply with applicable legal obligations

We do NOT sell your data. We do NOT use Client Data for advertising. We do NOT share Client Data between organizations on the Platform.

3. How We Share Your Information

3.1 Service Providers

We share information with trusted providers contractually bound to use your data only as directed by us:

- Supabase, Inc. — database, authentication, and file storage (supabase.com/privacy)
- Vercel, Inc. — application hosting (vercel.com/legal/privacy-policy)
- Stripe, Inc. — payment processing (stripe.com/privacy)
- Postmark/ActiveCampaign — transactional email (postmarkapp.com/privacy-policy)
- Sentry — error monitoring (sentry.io/privacy)

3.2 Legal Requirements

We may disclose information if required by law, regulation, legal process, or governmental request.

3.3 Business Transfers

In a merger, acquisition, or asset sale, your information may be transferred. We will notify you before your information becomes subject to a different privacy policy.

3.4 No Sale of Data

We do not sell, rent, or trade personal information or Client Data to third parties for commercial purposes. This applies to all users including those with rights under the CCPA/CPRA.

4. Data Storage and Security

4.1 Storage Location

Data is stored on servers in the United States. International data residency options are planned for future releases.

4.2 Security Measures

We implement:

- TLS 1.2+ encryption for all data in transit (HTTPS)
- AES-256 encryption for data at rest
- Row-level security policies ensuring organizational data isolation at the database level
- SOC 2 Type 2 certified authentication provider
- Access to production systems restricted to authorized MPC Solutions personnel
- Automated daily database backups retained for a minimum of 7 days

4.3 Data Breach Notification

In the event of a confirmed breach affecting your Client Data, we will notify your administrator by email within 72 hours of confirmation, to the extent required by applicable law.

5. Data Retention

We retain Client Data as long as your account is active. Upon termination, data is available for export for 30 days, then permanently deleted from active systems within 60 days. Backup copies may persist up to 90 additional days before permanent deletion.

Billing records and communications may be retained longer as required by law or for legitimate business purposes.

6. Your Rights and Choices

6.1 Access and Correction

You may access and update account information through your account settings. Contact support@mpcsolutions.org for assistance.

6.2 Data Export

Export Client Data at any time using the Platform's built-in tools (CSV, Excel, PDF). We will also assist with export requests sent to support@mpcsolutions.org.

6.3 Account Deletion

Request deletion of your account and all Client Data by contacting support@mpcsolutions.org. Requests are processed within 30 days, subject to legal obligations.

6.4 Email Communications

Opt out of non-transactional emails via the unsubscribe link in any such email. You cannot opt out of transactional emails necessary for account operation.

6.5 California Privacy Rights (CCPA/CPRA)

California residents have the right to: (a) know what personal information we collect; (b) request deletion; (c) opt out of sale of personal information (we do not sell); and (d) non-discrimination for exercising privacy rights. Contact support@mpcsolutions.org.

6.6 Rights of End Subjects

Individuals whose information is stored by our Clients (donors, volunteers, participants) should direct requests to the relevant Client organization. We will cooperate with Clients in responding as required by law.

7. Cookies and Tracking Technologies

The Platform uses cookies for session management, preferences, and analytics. We use:

- Essential cookies: Required for Platform operation including session authentication. Cannot be disabled.
- Analytics cookies: Help us understand Platform usage. May be disabled through your browser settings.

We do not use advertising cookies or track users across third-party websites. We do not participate in ad networks.

8. Children's Privacy

The Platform is not directed at children under 13. We do not knowingly collect information from children under 13. Contact support@mpcsolutions.org immediately if you believe we have done so.

If your programs serve minors, you are responsible for obtaining all required parental or guardian consents and ensuring compliance with COPPA and other applicable laws.

9. HIPAA Notice

The Platform is not certified as a HIPAA-compliant platform. If your organization handles protected health information (PHI) as defined by HIPAA, do not store such information in the Platform without first entering into a Business Associate Agreement (BAA) with MPC Solutions. Contact support@mpcsolutions.org to discuss HIPAA requirements.

10. Changes to This Privacy Policy

We may update this Policy periodically. We will notify you of material changes by email to your administrator address at least 30 days before changes take effect. Continued use constitutes acceptance.

11. Contact Us

MPC Solutions, LLC

Attn: Privacy Support

762 Burlwood Street, Brandon, Florida 33511

Email: support@mpcsolutions.org

Website: mpcsolutions.org

We will respond to all privacy inquiries within 30 days.