

Spellboundcoaching Privacy Policy Analysis

Source: <https://www.spellboundcoaching.com/pages/policies>

Analyzed: December 29, 2025 at 11:32 PM

Privacy Scorecard

Overall Grade: F

Privacy Score: 58/100

Third-Party Sharing (20%):

4/10

The policy allows broad sharing with third-party advertisers and social media platforms for behavioral tracking and targeted marketing, which is less protective than industry best practices.

User Rights & Control (18%):

6/10

While it explicitly mentions GDPR rights for EU users and CalOPPA compliance, the process for non-EU users to exercise rights like deletion is less clearly defined.

Data Collection (18%):

7/10

Collection is standard for e-commerce and coaching services, though the use of automated tracking technologies for behavioral analysis is relatively broad.

Data Retention (14%):

5/10

Retention is defined by vague criteria such as 'until the company decides it no longer needs the data,' lacking specific timeframes or automated deletion schedules.

Purpose Clarity (12%):

7/10

Primary purposes for data use are clearly linked to service delivery and marketing, though 'improving Site experience' remains a somewhat broad catch-all.

Security Measures (10%):

6/10

The policy mentions SSL and secured networks but lacks technical depth regarding encryption at rest or specific audit standards.

Policy Transparency (8%):

7/10

The policy is well-organized with clear headings and a 'Last Updated' date, though it contains standard legal language rather than a simplified layered format.

Key Concerns:

- Indefinite data retention based on subjective 'value' to the company rather than fixed periods.
- Extensive use of third-party behavioral tracking and pixels for social media advertising.
- The 14-day data breach notification window may be slower than the 'without undue delay' standard expected in high-protection frameworks.

Positive Aspects:

- Explicitly grants GDPR rights to users within the European Union, including rights to access and erasure.
- Clear opt-out instructions for Google Analytics and email marketing are provided.

Policy Summary

Privacy Analysis Report: Spellbound Coaching LLC

Executive Summary

This report analyzes the combined Terms & Conditions, Privacy Policy, and Shop Policies of Spellbound Coaching LLC. The company provides somatic intimacy coaching, disability coaching, and physical merchandise. The privacy stance is typical for a small e-commerce and service-based business: it relies heavily on third-party processors (Shopify, Google, and social media platforms) for data handling while maintaining a standard level of transparency regarding what is collected.

Overall, the policy is moderately privacy-friendly. While it explicitly states that it does not sell personal information for marketing purposes, it utilizes extensive tracking technologies (cookies and pixels) for targeted advertising on social media. A significant point of note is the heavy legal protection the company maintains through mandatory arbitration and a total waiver of jury trials for any disputes, including those involving data.

Readability Assessment

- **Language:** The document uses a mix of plain language and standard legal templates. While the Privacy Policy section is relatively clear, the Terms of Service are dense with legal jargon regarding liability and arbitration.
- **Structure:** Key points are organized under bold headers, making it relatively easy to navigate. However, privacy information is spread across three different documents (Terms, Privacy Policy, and Shop Policies), which may lead to user confusion.
- **Length:** The document is moderately long but comprehensive.
- **Verdict:** Moderately Clear. A layperson can understand the data collection sections, but the legal implications of the arbitration and liability clauses require careful reading.

Data Collection Sensitivity

- **Information Provided Directly:** Names, email addresses, mailing addresses, and payment/credit card information.
- **Automatically Collected Data:** IP addresses, geographic location, browser type, device info, and site behavior (via Google Analytics).
- **Sensitive Data Categories:** Financial data (processed via third parties) and potentially sensitive health/lifestyle information, given the nature of "somatic intimacy coaching."
- **Collection Necessity:** Collection appears limited to what is necessary for order fulfillment and marketing.
- **Sensitivity Assessment:** Moderate. While they don't collect biometric data, the nature of the coaching services may involve users sharing sensitive personal history via contact forms or sessions.

Data Sharing & Third Parties

- **Recipients:** Service providers (Shopify, email marketing), Data Collection Companies (Google Analytics), Social Media platforms (Facebook, Instagram, Pinterest, Bluesky), and Law Enforcement (if required).
- **Selling Data:** The policy explicitly states they do not sell or trade personal information to outside parties for marketing.
- **Sharing Context:** Data is shared to facilitate transactions, improve site performance, and run targeted "retargeting" ads on social media.
- **International Transfers:** Not explicitly detailed, though the use of US-based services (Google, Shopify) implies data resides in or passes through the US.
- **Sharing Assessment:** Limited Sharing. Sharing is primarily functional (payment/shipping) or for the company's own marketing efforts.

Complexity of User Controls

- Opt-Out Process: Users can opt-out of emails via an "Unsubscribe" link. Opting out of cookies requires manual browser adjustment or using the site's cookie banner.
- Data Deletion: There is no automated "Delete My Data" button. Users must email the owner () to request corrections or updates.
- Dark Patterns: None identified; the unsubscribe and contact info are clearly labeled.
- Complexity Assessment: Moderate effort required. Most actions require a direct email request rather than self-service settings.

Data Retention & Storage

- Duration: Personal information is kept until the user asks for deletion or the company decides the cost of retention outweighs the value.
- Account Closure: The policy does not specify an automatic deletion trigger upon account closure.
- Data Export: Not explicitly mentioned as a general right for all users (only implied for EU/GDPR users).
- Retention Assessment: Extended Retention. The policy leans toward keeping data as long as it remains useful to the business.

User Rights

- Standard Rights: Users can request to update or correct incorrect information via email.
- GDPR Rights: EU users are specifically granted rights to access, erase, and rectify data, as well as the right to lodge a complaint with a supervisory authority.
- California Rights (CalOPPA): Users are notified that they can visit the site anonymously and will be notified of policy changes on the privacy page.

Security Measures

- Protections: Use of SSL (Secure Sockets Layer) certificates and secured networks.
- Payment Security: Credit card information is never sent via email and is handled by third-party gateway providers (not stored on the company's servers).
- Breach Notification: The company commits to notifying users via email within 14 business days of a known data breach.

Children's Privacy

- Age Limit: The service is strictly for individuals 18 years or older.
- COPPA Compliance: They do not knowingly market to or collect data from children under 13. Parents are encouraged to contact the company for immediate data removal if a child provides info.

Policy Changes

- Notification: Changes are posted directly to the Privacy Policy page.
- Identification: Users must check the "Updated on" date at the bottom of the page to identify changes. No proactive notification (like a popup or email) is guaranteed for minor changes.

Key Concerns & Red Flags

- Arbitration & Jury Waiver: Users waive their right to a jury trial and are forced into binding arbitration in Maryland for any disputes, including those regarding privacy.
- Social Media Tracking: Extensive use of pixels (Facebook, Instagram, etc.) means your browsing habits on this site are shared with major social media networks for advertising purposes.
- Vague Retention: The criteria for keeping data ("until the Company decides it no longer needs the data") is subjective and gives the user little certainty.
- Third-Party Liability: The policy repeatedly disclaims liability for the actions of third-party links or payment processors.

Positive Aspects

- **No Selling of Data:** A clear commitment not to sell personal info to third-party marketers.
- **Transparent Contact:** The owner provides a direct email and physical business address for privacy inquiries.
- **Breach Commitment:** A specific 14-day timeline for breach notification is more transparent than many small-business policies.

Recommendations for Users

1. **Use Privacy Tools:** If you do not want your visit tracked for Facebook ads, use a browser with tracker blocking (like Brave) or an extension like uBlock Origin.
2. **Payment Choice:** Use a masked card service or a third-party processor like PayPal or Apple Pay to avoid sharing your primary credit card details directly with the platform.
3. **Exercise GDPR/CCPA Rights:** Even if you aren't in the EU or California, email the company to request data deletion if you no longer use the service.
4. **Sensitive Info:** Be cautious about the amount of personal detail you include in "Contact" or "Inquiry" forms, as this data is stored in their email/database systems.

Privacy Risks (6)

Waiver of Jury Trial and Class Action Rights

[Higher Risk]

The terms require all disputes to be resolved through binding arbitration in a specific location (Maryland), and users explicitly waive their right to a jury trial and the ability to seek punitive damages.

Reporting Chargebacks to Credit Bureaus

[Higher Risk]

The company threatens to report any credit card chargebacks to major credit reporting agencies, which could negatively impact the user's credit score.

Extensive Liability Release and Indemnification

[Higher Risk]

Users agree to release the company from all liability for harm, including death or injury, and agree to pay for the company's legal defense if a claim arises from the user's actions.

Broad License to Use User Content

[Medium Risk]

By commenting or submitting documents, users grant the company a perpetual license to use that information in any way the business sees fit.

Third-Party Behavioral Tracking and Ad Targeting

[Medium Risk]

The site shares user behavior and actions with third-party social media platforms (Facebook, Instagram, etc.) to track interests and serve targeted advertisements.

Health and Allergy Risk Disclosure

[Medium Risk]

The company is not a licensed medical professional, yet sells products produced in environments containing allergens (pets, smoke) and provides health-related coaching.

Key Terms Glossary (10)

Arbitration Clause

A requirement to settle legal disputes through a neutral third-party (arbitrator) instead of a judge or jury trial.

Personal Information

Data that can identify you specifically, such as your name, email, physical address, or phone number.

Cookies

Small data files stored on your computer that help a website remember your preferences and tracking your site activity.

Limited Licensee

A status given to users that allows them to view or use the company's materials for personal use only, without owning them.

Indemnification

An agreement where you promise to pay for any losses or legal costs the company faces because of your actions or breach of the terms.

SSL certificate

A digital security technology that creates an encrypted link between a website and a browser to keep data transfers private.

Pixels

Tiny snippets of code used to track how you interact with a website, often used to show you targeted ads on social media.

Severability

A legal rule stating that if one part of the agreement is found to be invalid, the rest of the agreement remains in effect.

Governing Law

The specific state laws (in this case, Maryland) that will be used to interpret the agreement and settle any disputes.

GDPR Rights

Privacy protections for individuals in the European Union, including the right to access, fix, or delete their personal data.