



BELZY LLC

Where Real Connections Begin

PRIVACY POLICY

Enterprise Data Protection, Security & Privacy Operations Framework

*Global US/GDPR / UK US/GDPR / CCPA-CPRA / U.S. State Law / Biometric Privacy
Compliance Edition*

Version 2.0



1. Introduction and Acceptance of This Policy	3
4.1 Information You Provide Directly	5
4.2 Information Collected Automatically	6
4.3 Information From Third Parties	6
4.4 Inferred and Derived Information	6
5.1 Biometric-Specific Disclosures (Illinois BIPA / Texas CUBI / Washington Biometric Law)	7
6. How We Use Your Information	8
7. Legal Bases for Processing (US/GDPR / UK US/GDPR)	8
9. How We Disclose Your Information	9
9.1 With Other Users	9
9.2 With Service Providers / Processors	10
9.3 For Safety and Legal Reasons	10
9.4 Business Transfers	11
9.5 Corporate Affiliates	11
9.6 Advertising Partners	11
9.7 Aggregated and De-Identified Data	11
10. Categories of Personal Information Disclosed for a Business Purpose (Prior 12 Months)	11
11. “Sale” and “Sharing” of Personal Information; Your Opt-Out Rights	12
12. Virtual Rooms, Messaging, and Real-Time Communications	12
13. Safety Features, Identity Verification, and Content Moderation	12
14. Cookies, SDKs, Pixels, and Similar Tracking Technologies	13
15. Data Retention and Deletion Schedule	13
16. Data Security Program	14
17. International Data Transfers	14
18. Your Privacy Rights — Global Overview	15
19. European Economic Area, United Kingdom, and Switzerland (US/GDPR / UK US/GDPR)	15
20. California Privacy Rights (CCPA / CPRA)	15
20.1 Your Rights	15
20.2 Submitting a Request	16
20.3 Shine the Light	16
21. Other U.S. State Privacy Rights	16
22. Illinois, Texas, and Washington — Biometric-Specific Rights	17
23. Nevada Privacy Rights	18
24. Children's Privacy and Minimum Age Requirement	18
25. International Users Outside the United States	18
26. Marketing Communications and Choices	18
27. Third-Party Links, Social Logins, and Integrations	19



28. Data Breach Notification	19
29. Privacy Governance, Impact Assessments, and Training	19
30. Do Not Track Signals and Global Privacy Control	19
31. Changes to This Privacy Policy	19
32. Governing Law and Dispute Resolution	19
33. Contact Us	20

1. Introduction and Acceptance of This Policy

Belzy, Inc., together with its subsidiaries and corporate affiliates ("Belzy," "we," "us," or "our"), provides the Belzy mobile application, the website at thebelzy.com, and related features and services (collectively, the "Service"). This Privacy Policy ("Policy") describes, in detail, the categories of personal information we collect, the sources and purposes of that collection, how we use, disclose, and safeguard personal information, the rights available to you under applicable law, and how to exercise those rights.

Belzy is a dating and social-connection platform. Because the Service inherently involves identity verification, biometric liveness checks, real-time video and audio interaction, precise location, and information about your intimate preferences and personal life, this Policy has been drafted to meet or exceed the disclosure standards applied by major dating platforms — to align with the requirements of the USA, EU/UK General Data Protection Regulation ("US/GDPR"), the California Consumer Privacy Act as amended by the California Privacy Rights Act ("CCPA/CPRA"), the twenty-plus comprehensive U.S. state consumer privacy laws currently in effect, sector-specific biometric privacy statutes (Illinois BIPA, Texas CUBI, and Washington's biometric law), and comparable international data-protection frameworks.

By creating a Belzy account or otherwise accessing or using the Service, you confirm that you have read, understood, and agree to the practices described in this Policy. If you do not agree with this Policy, you must not access or use the Service. This Policy is incorporated by reference into, and should be read together with, Belzy's Terms of Service, Community Guidelines, and Cookie Policy.



2. Definitions

- “Personal Information” / “Personal Data” means any information that identifies, relates to, describes, or could reasonably be linked, directly or indirectly, with a particular individual or household.
- “Sensitive Personal Information” / “Special Category Data” means personal information that receives heightened protection under applicable law, including but not limited to precise geolocation, racial or ethnic origin, religious or philosophical beliefs, sex life or sexual orientation, health information, biometric information used for identification, and government identification numbers.
- “Biometric Identifier/Information” means data generated from measurements of an individual's unique biological characteristics, such as a faceprint or facial geometry derived from a selfie or liveness scan, used to verify or identify an individual.
- “Processing” means any operation performed on personal information, including collection, storage, use, disclosure, and deletion.
- “Controller” / “Business” means the entity that determines the purposes and means of processing personal information; “Processor” / “Service Provider” means an entity that processes personal information on the Controller's behalf and under its instructions.
- “Sale” and “Share,” as used in Sections 10–11, have the meanings given under the CCPA/CPRA and analogous U.S. state privacy laws.
- “Virtual Room” means Belzy's synchronous shared-activity features, including Movie Nights, Truth or Dare, Ice Breaker Questions, Virtual Dinner, and similar experiences.

3. Scope, Applicability, and Our Role as Data Controller

This Policy applies to all personal information processed in connection with: the Belzy mobile application (iOS and Android) and thebelzy.com; account registration, identity verification, and profile creation; matching, messaging, audio/video calling, and Virtual Room features; AI-powered features, including AI Companion and AI Relationship Coach; and customer support, safety operations, and Premium subscription billing.

For most processing described in this Policy, Belzy, Inc. acts as the data controller (or “business” under U.S. state law) responsible for determining why and how your personal information is processed. Where Belzy processes information on behalf of another party, or where a vendor processes information on Belzy's behalf and under its instructions, that vendor acts as a processor/service provider, as described in Section 9.2. This Policy does not apply to third-party websites, applications, or integrations that may be linked from the Service; those third parties maintain their own privacy notices.



4. Information We Collect

We collect personal information in four ways: information you provide directly, information collected automatically through your use of the Service, information we receive from third parties, and information we derive or infer from the foregoing.

4.1 Information You Provide Directly

Category	Examples	Collected When
Account & Registration	Name, date of birth, gender, sexual orientation/preference, email, phone number, password	Sign-up
Profile Content	Photos, bio, interests, relationship goals, prompts, height, education, occupation, lifestyle choices	Profile creation/editing
Identity Verification	Government-issued ID image, selfie/liveness biometric scan, Verified Badge status	Verify Your Identity flow
Communications	Messages, call metadata, Virtual Room responses (e.g., Truth or Dare answers), reports about other users	Ongoing use of the Service
Safety Preferences	Emergency contact information and safety-check preferences, where you choose to enable such features	Optional safety settings
Customer Support	Correspondence, complaint details, safety-report content, appeals	Contacting support
Payment Information	Billing name, tokenized payment method, transaction history (full card numbers are processed and stored only by our payment processor)	Premium subscription purchase



4.2 Information Collected Automatically

Category	Examples	Collected Via
Device & Technical Data	Device model, OS, unique device and advertising identifiers, IP address, browser type, mobile carrier	SDKs / server logs
Usage Data	Features used, swipes/likes, match activity, session length and frequency, crash logs, diagnostics	App instrumentation
Location Data	Precise or approximate geolocation (with permission), IP-inferred location, distance shown to other members	Device location permission
Cookies & SDKs	Cookies, mobile ad identifiers, pixel tags, analytics/attribution SDKs	See Section 14

4.3 Information From Third Parties

- Single sign-on providers (e.g., Apple, Google, Facebook), if you register or log in through them;
- Other users, through reports, blocks, or shared communications submitted for moderation review;
- Identity-verification and fraud-prevention vendors confirming document authenticity and biometric liveness;
- Payment processors, confirming transaction status;
- Analytics, advertising, and attribution partners, consistent with your consent and applicable law;
- Publicly available sources, where relevant to safety investigations (for example, verifying sanctioned or registered-offender status where legally required and available).

4.4 Inferred and Derived Information

We generate certain information by analyzing the categories above — for example, compatibility scores, engagement patterns, likely interests, and fraud-risk signals. This inferred information is used for the purposes described in Section 6 and is treated with the same protections as the underlying data from which it was derived.



5. Sensitive Personal Information and Biometric Data

Certain information processed by Belzy is classified as “sensitive personal information” or “special category data” under applicable law, including: precise geolocation; sexual orientation and dating preferences; religious or philosophical beliefs you choose to disclose; health information you voluntarily share; government identification numbers or images; and biometric identifiers derived from your identity-verification selfie or liveness scan (“Face Data”). We process this information only where you have provided it voluntarily and where processing is necessary to operate core features (matching, verification, and safety), and it is subject to the heightened security controls described in Section 16.

5.1 Biometric-Specific Disclosures (Illinois BIPA / Texas CUBI / Washington Biometric Law)

When you complete Belzy's optional photo/selfie identity-verification flow, we (or our identity-verification vendor, acting on our behalf) capture a biometric identifier — a mathematical representation of your facial geometry (“Face Data”) — and compare it against your submitted government ID and/or existing profile photos to confirm you are a real, unique person.

- **Purpose:** Face Data is collected and used solely to verify your identity, issue or maintain your Verified Badge, and detect duplicate or fraudulent accounts.
- **Consent:** Where required by law (including Illinois BIPA and Washington's biometric statute), we obtain your informed, written consent through a dedicated verification consent screen before capturing Face Data — separate from general Terms of Service acceptance.
- **Retention & Destruction:** Face Data is retained only as long as necessary to complete verification and to support ongoing fraud-prevention and duplicate-account detection, and in any event is deleted or irreversibly de-identified no later than three (3) years after your last authenticated use of the Service, or sooner upon a verified deletion request, whichever occurs first.
- **No Sale or Unauthorized Disclosure:** We do not sell, lease, trade, or otherwise profit from biometric identifiers, and we disclose Face Data only to our identity-verification processor (acting under contract and solely to perform verification on our behalf), or where required by law, valid legal process, or with your consent.
- **Your Rights:** Where applicable law provides a private right of action or statutory remedy for biometric-data violations (such as Illinois BIPA), nothing in this Policy is intended to waive those rights except to the extent permitted by law.



6. How We Use Your Information

The table below summarizes our primary processing purposes and, where the US/GDPR/UK US/GDPR applies, the corresponding legal basis (see Section 7 for a fuller explanation of each basis).

Purpose	Legal Basis (US/GDPR/UK US/GDPR)
Create and operate your account and profile	Contractual necessity
Operate AI-powered matching and profile ranking	Contractual necessity / Legitimate interests
Enable messaging, calls, and Virtual Room features	Contractual necessity
Power AI Companion and AI Relationship Coach (Premium)	Consent / Contractual necessity
Verify identity and issue the Verified Badge	Consent (biometric) / Legitimate interests (safety)
Detect fraud, fake accounts, and bots	Legitimate interests / Legal obligation
Investigate reports and enforce Community Guidelines	Legitimate interests / Legal obligation
Process Premium subscription payments	Contractual necessity
Send service and security notifications	Contractual necessity / Legitimate interests
Send marketing communications	Consent (opt-in) / Legitimate interests where permitted
Analyze aggregate trends to improve the Service	Legitimate interests
Comply with law and respond to legal process	Legal obligation

7. Legal Bases for Processing (US/GDPR / UK US/GDPR)

Where the US/GDPR or UK US/GDPR applies to our processing of your personal data, we rely on one or more of the following legal bases:

- Contractual necessity — to create your account and provide core matching, messaging, and Virtual Room functionality;



- Consent — for biometric identity verification, optional sensitive-profile disclosures, marketing communications, and certain cookies/SDKs; you may withdraw consent at any time without affecting the lawfulness of processing before withdrawal;
- Legitimate interests — for fraud prevention, platform safety, product analytics, and direct marketing to existing users, always balanced against your rights and reasonable expectations;
- Legal obligation — where processing is required to comply with applicable law or a lawful request from a public authority.

You may request further information about the specific legal basis relied upon for a given processing activity by contacting privacy@thebelzy.com.

8. AI-Powered Features and Automated Decision-Making

Belzy uses artificial intelligence and machine-learning systems to power several features:

- Algorithmic Matchmaking — ranks and suggests profiles based on stated preferences, in-app behavior, and compatibility signals;
- AI Fraud Detection — flags suspicious accounts, images, or messaging patterns for human review;
- AI Companion and AI Relationship Coach (Premium) — generates conversational prompts, icebreakers, and coaching suggestions based on your activity and stated preferences.

These systems influence which profiles you see and support content-moderation triage, but any decision with a legal or similarly significant effect on you — such as a permanent account suspension for a safety violation — is subject to human review before being finalized. Where required by applicable law, you may: (a) request a meaningful explanation of the logic involved in an automated decision that significantly affects you; (b) object to, or request not to be subject to, solely automated decision-making; and (c) request human review of such a decision. To exercise these rights, contact privacy@thebelzy.com.

9. How We Disclose Your Information

We do not sell your personal information for money. We disclose personal information only in the circumstances described below; Section 11 separately addresses activities that may constitute a “sale” or “share” under certain U.S. state laws even though no money changes hands.

9.1 With Other Users

Your profile (photos, bio, prompts, Verified Badge, approximate distance, and shared Virtual Room activity) is visible to other users as part of the Service's core functionality, based on the visibility settings you select.



9.2 With Service Providers / Processors

We engage vetted vendors to perform services on our behalf, under contractual confidentiality, security, and data-protection obligations that restrict their use of your information to providing services to Belzy. Current categories of sub-processors include:

Sub-Processor Category	Function
Cloud Hosting & Infrastructure	Application hosting, database storage, content delivery
Identity Verification & Biometric Liveness	Government ID validation, selfie/liveness matching for the Verified Badge
Payment Processing	Premium subscription billing, transaction fraud screening
Customer Support Platform	Ticketing, in-app help, safety-report workflow
Product Analytics & Crash Reporting	Feature usage measurement, stability monitoring
Push Notification & Messaging Delivery	Match alerts, message alerts, security notifications
AI/ML Model Providers	Matching-algorithm inference, AI Companion and AI Relationship Coach conversational features
Content Moderation Tooling	Automated image/text screening, report triage
Marketing & Attribution	Campaign measurement, opt-in marketing communications (where consented)
Email/SMS Delivery	Transactional and, where opted in, marketing messages

A current, itemized list of named sub-processors is available upon request to privacy@thebelzy.com and, where required by the US/GDPR's cross-border transfer rules, will be maintained as an appendix to our Data Processing Agreements.

9.3 For Safety and Legal Reasons

- To investigate or respond to reports of harassment, fraud, or safety concerns, including sharing information with other dating platforms' cross-industry safety coalitions where permitted by law;
- To comply with subpoenas, court orders, or other valid legal process;
- To protect the rights, property, or safety of Belzy, our users, or the public, including where there is a good-faith belief of harm to a minor or a credible threat of violence.



9.4 Business Transfers

If Belzy is involved in a merger, acquisition, financing, reorganization, or sale of assets, personal information may be transferred as part of that transaction, subject to standard confidentiality protections and, where required by law, advance notice to affected users.

9.5 Corporate Affiliates

We may share information among Belzy's corporate affiliates for the purposes described in this Policy, including shared safety and fraud-prevention infrastructure, subject to the same protections described here.

9.6 Advertising Partners

Where you have not opted out (see Section 11), we may allow advertising partners to collect information via cookies or SDKs, or we may disclose limited information to them, to measure and improve the relevance of ads. See Sections 11 and 14 for your choices.

9.7 Aggregated and De-Identified Data

We may share aggregated or de-identified information that cannot reasonably be used to re-identify you, such as industry trend reporting or research collaborations.

10. Categories of Personal Information Disclosed for a Business Purpose (Prior 12 Months)

The table below reflects the general categories of personal information that CCPA/CPRA-covered businesses in the dating-app industry typically disclose to service providers or other categories of third parties for a business purpose, consistent with the categories defined in Cal. Civ. Code § 1798.140. Belzy will confirm and finalize the accuracy of this table against its actual disclosures prior to publication.

Category of Personal Information	Disclosed To	Business Purpose
Identifiers (name, email, device ID)	Service providers, affiliates	Account operation, security
Profile & preference data	Other users, service providers	Matching, Service functionality
Precise geolocation	Service providers	Distance-based matching
Biometric information (Face Data)	Identity-verification processor	Identity verification, fraud prevention



Sensitive characteristics (sexual orientation, etc.)	Service providers (as necessary)	Matching, Service functionality
Commercial information (transaction history)	Payment processor	Billing, fraud prevention
Internet/network activity	Analytics & advertising partners	Analytics, advertising (opt-out available)
Audio/visual information (photos, call metadata)	Other users, service providers	Service functionality, moderation

11. “Sale” and “Sharing” of Personal Information; Your Opt-Out Rights

Belzy does not sell personal information in exchange for money. However, if Belzy uses cookies, SDKs, or similar technology to allow advertising partners to collect information for cross-context behavioral advertising, that activity may be considered a “sale” or “share” under the CCPA/CPRA and similar laws, even without a monetary exchange.

- You may opt out of any such sale/sharing at any time via the “Your Privacy Choices” link in the app footer or Settings menu;
- Where required by law, Belzy will honor the Global Privacy Control (“GPC”) signal and other recognized Universal Opt-Out Mechanisms as a valid opt-out request from supported browsers/devices;
- We do not knowingly sell or share the personal information of users under 18 (the Service is not directed to, and is not available to, anyone under 18); and
- Opting out of sale/sharing will not affect your ability to use core Service features, and we will not discriminate against you for exercising this right.

12. Virtual Rooms, Messaging, and Real-Time Communications

Virtual Room features (Movie Nights, Truth or Dare, Ice Breaker Questions, Virtual Dinner, Draw Together, Plan Your Future Trip, and similar experiences) involve real-time, synchronous interaction between matched users. Content exchanged in Virtual Rooms — including game responses, chat messages, and session metadata — is stored to enable the feature to function, to support moderation and safety review if a report is filed, and, where you consent, to improve matching and engagement features. Audio/video calls are encrypted in transit; Belzy does not record audio/video calls by default. Either participant may report content shared in a Virtual Room, which is reviewed under Section 9.3.

13. Safety Features, Identity Verification, and Content Moderation

Belzy offers optional and mandatory safety features designed to reduce fraud, impersonation, and harmful conduct on the platform:



- Photo & ID Verification — confirms that your profile photos match a real, government-issued ID via the biometric process described in Section 5.1;
- AI Fraud Detection — automated screening for bot activity, duplicate accounts, and known scam patterns, paired with human review;
- Report-Based Moderation — every user report is reviewed by Belzy's Trust & Safety team, and accounts found to violate our Community Guidelines may be restricted, suspended, or permanently banned;
- Optional Safety-Check Tools — where enabled by you, features such as emergency-contact sharing for in-person dates process the limited information necessary to operate that specific tool and are never used for matching or advertising purposes.

Belzy's verification and fraud-prevention processes are designed to reduce, but cannot eliminate, the risk of encountering a bad actor, and Belzy does not conduct criminal background checks unless explicitly stated as a distinct, separately-consented feature.

14. Cookies, SDKs, Pixels, and Similar Tracking Technologies

We and our service providers use cookies, mobile SDKs, pixels, and similar technologies to:

- Keep you logged in and remember preferences (strictly necessary — cannot be disabled without impairing core functionality);
- Understand feature usage and app performance (analytics);
- Measure the effectiveness of, and where applicable personalize, marketing campaigns (advertising), only with consent where required by law.

You can manage browser cookie preferences through your browser settings, and manage mobile advertising identifiers through your device's privacy settings (e.g., “Limit Ad Tracking” / “Opt out of Ads Personalization”). Where required by law, we present a cookie-consent banner allowing you to accept or reject non-essential cookies, and we honor GPC and other recognized opt-out signals as described in Section 11. Further detail is available in our separate Cookie Policy.

15. Data Retention and Deletion Schedule

Data Category	Retention Period	Rationale
Account & profile data	Duration of account, plus up to 90 days after deletion	Fraud/duplicate-account prevention
Verification documents (government ID)	Deleted promptly after verification is confirmed, subject to a limited fraud-prevention window	Identity assurance, legal obligation
Biometric Face Data	Deleted or irreversibly de-identified no later than 3 years after last authenticated use, or sooner on request	Biometric law compliance (Sec. 5.1)



Messages & Virtual Room content	Duration of account; extended if subject to an active safety report or legal hold	Service functionality, safety investigations
Payment records	Up to 7 years, as required by tax/financial regulation	Legal/accounting obligation
Support tickets & safety reports	Up to 3 years after resolution	Safety trend analysis, legal defense
Cookies & ad identifiers	Per cookie/SDK, typically 13–24 months absent renewed consent	Analytics/advertising

When information is no longer needed for the purposes above, we securely delete, anonymize, or aggregate it. Deletion timelines may be extended where necessary to comply with a legal obligation, resolve a dispute, or enforce our agreements.

16. Data Security Program

Belzy applies layered technical and organizational safeguards designed to protect personal information against unauthorized access, disclosure, alteration, and destruction, including:

- Encryption in transit (TLS 1.2+) for all data transmitted between your device and our servers, including messages and call signaling;
- Encryption at rest for stored personal data, including verification documents and biometric templates;
- Role-based access controls and least-privilege principles restricting employee access on a need-to-know basis;
- Multi-factor authentication for internal systems handling user data;
- Automated AI Fraud Detection paired with manual review of flagged accounts;
- Regular penetration testing, vulnerability scanning, and independent third-party security audits, targeting recognized frameworks such as SOC 2 and ISO/IEC 27001;
- A documented security-incident response plan, including notification to affected users and regulators within the timeframes required by applicable breach-notification law;
- Employee background checks and mandatory privacy/security training for personnel with data access;
- Community-driven, human-reviewed report-based moderation for every submitted safety report.

No method of transmission or storage is 100% secure, and we cannot guarantee absolute security. You play an important role in protecting your account by using a strong, unique password, enabling any available account-security features, and safeguarding your login credentials.



17. International Data Transfers

Belzy operates globally, and personal information may be transferred to, stored, and processed in countries other than your own, including the United States, where data-protection laws may differ from those in your jurisdiction. Where we transfer personal data out of the EEA, UK, or Switzerland, we rely on recognized transfer mechanisms, which may include: the European Commission's Standard Contractual Clauses; the UK International Data Transfer Addendum; participation in the EU-U.S. and Swiss-U.S. Data Privacy Framework, where applicable; or adequacy decisions, together with supplementary technical and organizational safeguards designed to ensure your data receives an equivalent level of protection wherever it is processed.

18. Your Privacy Rights — Global Overview

Depending on your place of residence, you may have some or all of the following rights: to know/access the personal information we hold about you; to correct inaccurate information; to delete your information; to receive a portable copy of your information; to restrict or object to certain processing, including profiling; to withdraw consent; to opt out of the sale/sharing of personal information and targeted advertising; to limit the use of sensitive personal information; and to lodge a complaint with a supervisory authority or regulator. Sections 19–23 below describe how these rights apply in specific jurisdictions.

19. European Economic Area, United Kingdom, and Switzerland (US/GDPR / UK US/GDPR)

If the US/GDPR or UK US/GDPR applies to you, you have the right to: access the personal data we hold about you; request correction of inaccurate data; request erasure (“right to be forgotten”); restrict or object to certain processing, including profiling used for matching (Section 8); request data portability; withdraw consent at any time without affecting the lawfulness of prior processing; and lodge a complaint with your local data-protection supervisory authority (in the UK, the Information Commissioner's Office).

20. California Privacy Rights (CCPA / CPRA)

20.1 Your Rights

- Right to Know / Access — request the categories and specific pieces of personal information collected, the categories of sources, the business/commercial purpose for collection, and the categories of third parties to whom it was disclosed;
- Right to Delete — request deletion of personal information we have collected, subject to certain legal exceptions;
- Right to Correct — request correction of inaccurate personal information;
- Right to Data Portability — receive a copy of specified personal information in a portable format;
- Right to Opt Out of Sale/Sharing — as described in Section 11;
- Right to Limit Use of Sensitive Personal Information — to what is reasonably necessary to provide the Service, including for Face Data (Section 5.1);
- Right to Non-Discrimination — we will not deny goods/services, charge different prices, or provide a different level of service because you exercised a CCPA right;



- Right to Appeal — if we decline to act on a request, you may appeal by replying to our denial notice or contacting privacy@thebelzy.com.

20.2 Submitting a Request

You may submit a Know, Delete, or Correct request through in-app account settings or by emailing privacy@thebelzy.com. We will verify your identity using information reasonably matched to what we already hold before fulfilling a request. You may designate an authorized agent to submit a request on your behalf, subject to identity- and authorization-verification. We will confirm receipt of verifiable requests within ten (10) business days and provide a substantive response within forty-five (45) calendar days, extendable by an additional forty-five (45) days where reasonably necessary, with notice to you.

20.3 Shine the Light

California residents may separately request, once per calendar year and free of charge, information about any personal information we may have disclosed to third parties for their own direct marketing purposes during the preceding calendar year, pursuant to California Civil Code § 1798.83. Belzy's practice is not to disclose personal information to third parties for their own direct marketing without your consent.

21. Other U.S. State Privacy Rights

Residents of the states listed below have rights that are broadly similar to those described in Section 20, subject to each statute's specific scope, thresholds, and exceptions. This table reflects the general landscape of comprehensive state privacy laws in effect as of 2026 and should be reviewed periodically as new laws take effect.

State	Statute	Core Consumer Rights
California	CCPA/CPRA	Know, delete, correct, port, opt out of sale/share & targeted ads, limit use of sensitive PI, non-discrimination, appeal
Virginia	VCDPA	Access, correct, delete, port, opt out of sale/targeted ads/profiling
Colorado	CPA	Access, correct, delete, port, opt out of sale/targeted ads/profiling; universal opt-out (GPC) required
Connecticut	CTDPA	Access, correct, delete, port, opt out of sale/targeted ads/profiling
Utah	UCPA	Access, delete, port, opt out of sale/targeted ads
Iowa	ICDPA	Access, delete, port, opt out of sale
Delaware	DPDPA	Access, correct, delete, port, opt out of sale/targeted ads/profiling



New Jersey	NJDPA	Access, correct, delete, port, opt out of sale/targeted ads/profiling
Oregon	OCPA	Access, correct, delete, port, opt out of sale/targeted ads/profiling
Montana	MTCDDPA	Access, correct, delete, port, opt out of sale/targeted ads/profiling
Texas	TDPSA	Access, correct, delete, port, opt out of sale/targeted ads/profiling; no revenue threshold
Nebraska	NDPA	Access, correct, delete, port, opt out of sale/targeted ads/profiling
New Hampshire	NHDPA	Access, correct, delete, port, opt out of sale/targeted ads/profiling
Minnesota	MNCDPA	Access, correct, delete, port, opt out of sale/targeted ads/profiling; right to question automated profiling
Maryland	MODPA	Access, correct, delete, port, opt out of sale/targeted ads; sale of sensitive PI prohibited outright
Indiana	INCDPA	Access, correct, delete, port, opt out of sale/targeted ads/profiling
Kentucky	KCDPA	Access, correct, delete, port, opt out of sale/targeted ads/profiling
Rhode Island	RIDTPPA	Access, correct, delete, port, opt out of sale/targeted ads/profiling
Arkansas	ADPA	Access, correct, delete, port, opt out of sale/targeted ads/profiling
Florida (qualifying entities)	FDBR	Access, correct, delete, port, opt out of sale/targeted ads/profiling
Nevada	NRS 603A	Right to opt out of the sale of covered information

To exercise rights under any of the laws listed above, contact privacy@thebelzy.com or use in-app privacy controls. Where a state law requires us to recognize a Universal Opt-Out Mechanism such as Global Privacy Control, we do so as described in Section 11.

22. Illinois, Texas, and Washington — Biometric-Specific Rights

In addition to the biometric disclosures in Section 5.1, residents of Illinois, Texas, and Washington have the following statute-specific protections:



- Illinois (BIPA) — written notice and written consent before collection of biometric identifiers; a publicly available retention/destruction schedule (see Section 15); a prohibition on profiting from biometric data; and, where applicable, a private right of action for statutory violations;
- Texas (CUBI) — informed consent before capture of a biometric identifier for a commercial purpose, a limited retention period, and destruction within a reasonable time after the purpose for collection has been satisfied; enforcement is by the Texas Attorney General;
- Washington (RCW 19.375) — notice and consent before enrolling a biometric identifier in a database for a commercial purpose, and a prohibition on sale/disclosure of biometric identifiers without consent; enforcement is by the Washington Attorney General.

23. Nevada Privacy Rights

Nevada residents have the right, under NRS 603A, to opt out of the sale of certain “covered information” to third parties for the third party's own direct marketing purposes. Belzy does not sell covered information in a manner that triggers this right; if that changes, we will provide a designated request mechanism as required by Nevada law.

24. Children's Privacy and Minimum Age Requirement

The Service is intended solely for individuals 18 years of age or older. We do not knowingly collect personal information from anyone under 18, and our identity-verification process (Section 5.1) is used, in part, to help enforce this restriction. If we learn we have collected personal information from a person under 18, we will promptly delete it and terminate the associated account. If you believe a minor is using the Service, please report it to trust@thebelzy.com.

25. International Users Outside the United States

If you access the Service from outside the United States, your information will be transferred to and processed in the United States and potentially other countries, as described in Section 17. In addition to the US/GDPR/UK US/GDPR protections described in Section 19, Belzy is committed to honoring applicable rights under other international frameworks, including but not limited to Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), Brazil's Lei Geral de Proteção de Dados (LGPD), and Australia's Privacy Act 1988. Residents of these and other jurisdictions may contact privacy@thebelzy.com to exercise applicable local rights.

26. Marketing Communications and Choices

Where you have opted in (or where permitted by law on an opt-out basis), we may send you marketing emails or push notifications about new features, promotions, or events. You may opt out at any time by using the “unsubscribe” link in marketing emails, adjusting push-notification permissions on your device, or updating your communication preferences in Settings. Opting out of marketing will not affect transactional or safety-related communications necessary to operate your account.



27. Third-Party Links, Social Logins, and Integrations

The Service may contain links to third-party websites or integrate third-party sign-on and payment services (e.g., Apple, Google, Facebook, and our payment processor). This Policy does not apply to those third parties, and we encourage you to review their respective privacy notices before connecting your account.

28. Data Breach Notification

In the event of a security incident involving unauthorized access to, or acquisition of, unencrypted personal information that triggers a notification obligation under applicable law, Belzy will notify affected individuals and, where required, relevant regulators or attorneys general without unreasonable delay and in accordance with the timeframes specified by applicable breach-notification statutes, and will provide information about the nature of the incident and recommended protective steps.

29. Privacy Governance, Impact Assessments, and Training

Belzy maintains an internal privacy governance program, which includes: conducting data protection impact assessments (DPIAs) for processing activities that present a heightened risk to individuals, such as large-scale processing of biometric or sensitive data and automated profiling; applying privacy-by-design and privacy-by-default principles when building new features; maintaining records of processing activities as required by applicable law; and providing mandatory privacy and security training to employees and contractors with access to personal information.

30. Do Not Track Signals and Global Privacy Control

Some browsers transmit “Do Not Track” signals; because there is no common industry standard for interpreting them, the Service does not currently respond to “Do Not Track” specifically. However, as described in Sections 11 and 14, we do honor the Global Privacy Control signal and other legally recognized Universal Opt-Out Mechanisms as valid opt-out-of-sale/share requests where required by law.

31. Changes to This Privacy Policy

We may update this Policy from time to time to reflect changes in our practices, technology, legal requirements, or other factors. We will post the updated Policy with a revised “Last Updated” date and, for material changes, provide additional notice (such as an in-app notification or email) prior to the change taking effect. Your continued use of the Service after the effective date of an update constitutes acceptance of the revised Policy.

32. Governing Law and Dispute Resolution



Except as otherwise required by applicable data-protection law (including mandatory consumer-protection provisions that cannot be waived by contract), this Policy is governed by the same governing-law and dispute-resolution provisions set out in Belzy's Terms of Service. Nothing in this Policy limits any non-waivable statutory right you may have under the law of your place of residence.

33. Contact Us

If you have questions, concerns, or requests regarding this Privacy Policy or our data practices, please contact:

Belzy, LLC. — Privacy & Data Protection Team

Email: privacy@thebelzy.com

Safety & Trust: trust@thebelzy.com