Family Law Software
A CENTERBASE COMPANY

Privacy Program

1. Introduction and Purpose

The primary purpose of this Privacy Program is to protect the personal information (PI) and sensitive client data that the Company processes and to ensure ongoing compliance with global data protection laws, including the **EU General Data Protection Regulation (GDPR)**, the **California Consumer Privacy Act (CCPA/CPRA)**, and any other relevant laws governing the legal technology sector.

The program is built on the principles of **Privacy by Design and Default** and is committed to transparency, accountability, and user control.

2. Scope

This policy applies to all systems, products, services, employees, contractors, and third-party vendors involved in the collection, use, storage, transmission, or disposal of Personal Information (PI) or Sensitive Personal Information (SPI).

Definitions:

- **Personal Information (PI):** Any information that can identify an individual (e.g., name, email, IP address, device ID).
- **Sensitive Personal Information (SPI):** PI that requires a higher level of protection, such as client matter details, financial information, health data (if applicable), or data categorized as sensitive under GDPR/CCPA.
- **Data Subject:** The identified or identifiable natural person to whom the PI relates.
- **Controller:** The entity that determines the purposes and means of processing PI (e.g., the Company for employee or website user data).
- **Processor:** The entity that processes PI on behalf of the Controller (e.g., the Company in relation to most of our legal firm clients' data).

3. Privacy Governance and Organization

3.1. Roles and Responsibilities

Role	Responsibility
Privacy Officer / Data Protection Officer (DPO)	Oversight of the entire Privacy Program. Serves as the primary point of contact for data subjects and supervisory authorities. Maintains the Record of Processing Activities (RoPA).
Data Owners	Senior management responsible for specific data sets (e.g., HR for employee data, Product for customer usage data). Accountable for data classification, retention, and access control.
Information Security Team	Implements and maintains technical and organizational security measures to protect PI against unauthorized access, disclosure, or breach.
All Employees	Adherence to all privacy policies, completion of mandatory annual privacy training, and immediate reporting of any potential privacy incident.

3.2. Record of Processing Activities (RoPA)

The DPO/Privacy Officer will maintain a detailed, up-to-date RoPA that documents:

- Categories of PI collected.
- The purpose of processing (and the legal basis for each purpose).
- Data retention periods.
- Categories of recipients with whom the data is shared.
- Details of international data transfers and the safeguards used.

4. Policy for Managing Personal Information (The Data Lifecycle)

4.1. Data Collection and Consent Policy

Principle	Requirement
Lawful Basis	PI will only be collected and processed if a clear, documented legal basis exists (e.g., performance of a contract, legitimate interest, or explicit consent).

Principle	Requirement
Data Minimization	Only the minimum amount of PI necessary to achieve the specified purpose will be collected. Data fields and collection processes must be regularly audited to enforce this.
Transparency (Notice)	A clear, accessible Privacy Policy will be published on the Company website and in the application detailing what PI is collected, how it is used, and the Data Subject's rights.
Explicit Consent	Where consent is the legal basis, it must be **freely given, specific, informed, and unambiguous**. Consent mechanisms must be granular, not pre-checked, and easy to withdraw.

4.2. Data Use and Processing Policy

Principle	Requirement
Purpose Limitation	PI will only be used for the explicit purposes disclosed to the Data Subject at the time of collection or a compatible purpose. Any secondary use requires a new legal basis or fresh consent.
Privacy by Design and Default	Privacy principles will be embedded into the entire Software Development Life Cycle (SDLC). The default setting for any new product or feature must be the most privacy-protective option.
Data Quality/Accuracy	Measures must be in place to ensure PI is accurate and, where necessary, kept up to date. Users must have mechanisms to request correction of inaccurate data.

4.3. Data Storage, Retention, and Disposal Policy

Principle	Requirement
Security	PI, especially SPI, must be protected by **encryption** both at rest and in transit. Access must be controlled via the **Principle of Least Privilege** and multi-factor authentication (MFA).
Storage Limitation	PI will be retained only for as long as necessary to fulfill the purpose for which it was collected or as required by law (e.g., legal hold, financial reporting).

Principle	Requirement
Secure Disposal	PI that has reached the end of its defined retention period must be securely deleted, destroyed, or fully anonymized/pseudonymized in a non-recoverable manner.

4.4. Third-Party Sharing and Vendor Management Policy

Principle	Requirement
Data Processing Agreements (DPAs)	All third-party vendors and partners who process PI on the Company's behalf must execute a legally compliant DPA that mandates security measures and adherence to this Privacy Program.
Due Diligence	Thorough privacy and security due diligence must be performed on all vendors before engagement and reviewed periodically.
International Transfers	Any transfer of PI across international borders (e.g., outside the EEA) must be done only through approved mechanisms, such as Standard Contractual Clauses (SCCs) or a recognized adequacy decision.

5. Data Subject Rights (DSR) Policy and Procedures

The Company is committed to honoring all applicable DSRs. A formal process and dedicated channels (e.g., a web form and toll-free number) will be provided for data subjects to exercise their rights.

Right	Description	Response Procedure
Right to Know/Access	The right to know what PI is collected, the sources of the data, the purpose of collection, and who it is shared with.	Acknowledge the request within **10 business days**. Provide the full response/data copy within **45 days** (extendable).
Right to Deletion	The right to request the deletion of PI, subject to certain legal exceptions (e.g., necessary for a contract, legal obligation).	Verify the Data Subject's identity. Fulfill the deletion request across all systems and notify relevant third parties within **45 days**.

Right	Description	Response Procedure
Right to Rectification	The right to have inaccurate or incomplete PI corrected without undue delay.	Investigate the claim and correct the inaccurate PI in all relevant systems within the statutory timeframe (e.g., **30 days** for GDPR).
Right to Opt-Out (Do Not Sell/Share)	The right to direct the business not to sell or share their PI for cross-context behavioral advertising (primarily CCPA/CPRA).	Implement a clear and conspicuous "Do Not Sell/Share My Personal Information" link on the Company homepage. Honor the request within **15 business days**.
Right to Restriction	The right to temporarily limit the processing of PI (e.g., while a claim of inaccuracy is being verified).	Segregate the data in question and limit processing to storage only until the restriction is resolved.
Right to Portability	The right to receive their PI in a structured, commonly used, machine-readable format and to transmit that data to another controller.	Provide the PI in a standard, easily readable format (e.g., CSV, JSON) within the statutory timeframe.

Export to Sheets

6. Privacy Incident Response

A formal Privacy Incident Response Plan is maintained and regularly tested.

- **Detection & Assessment:** Any security or privacy incident must be reported immediately to the DPO/Security Team.
- **Containment & Recovery:** Take immediate steps to contain the breach and restore system integrity.
- **Notification:** If a breach involves PI, the DPO will determine the necessity of notifying affected Data Subjects and/or relevant Supervisory Authorities (e.g., within **72 hours** for a GDPR reportable breach).
- **Post-Incident Review:** Conduct a thorough root cause analysis and update controls/policies to prevent recurrence.

7. Training and Awareness

All employees and contractors must complete mandatory, role-specific privacy and security training upon onboarding and at least annually thereafter. Training content will cover:

- The definition of PI and SPI.
- Employee responsibilities under this Privacy Program.
- Procedures for handling Data Subject Rights Requests.
- Protocols for identifying and reporting privacy incidents.