SimpleLegal and General Data Protection Regulation (GDPR)

What is General Data Protection Regulation (GDPR)?

The General Data Protection Regulation, commonly referred to as GDPR, is a new comprehensive data protection law in the EU going into effect on May 25, 2018. It regulates the processing of Personal Data including the collection, storage, transfer, and use of personal data about EU individuals.

GDPR applies to all organizations processing Personal Data of EU residents. Personal Data is any information relating to an identified or identifiable natural person.

Key GDPR Elements Include:

I. The Relationship Between Data Controllers and Data Processors
II. Types of Personal Data
III. Protection of Personal Data
IV. Transfer of Personal Data
V. Data Subject Consent
VI. Retention & The Right to be Forgotten

SimpleLegal has been working with legal experts to make sure we remain compliant with how we handle customer data, and have the tools necessary to help our customers properly manage their vendor / outside counsel data.

This information is meant to help our customers understand how we process Personal Data on their behalf and to help them with their compliance initiatives:

I. Data Controllers and Data Processors

GDPR includes obligations for both Data Controllers and Data Processors. SimpleLegal is the Data Processor responsible for storing and processing the Personal Data on behalf of our Customers. The Customer is the Data Controller with respect to Personal Data stored and processed on the SimpleLegal platform. The Customer owns the Personal Data processed by SimpleLegal and decides how that Personal Data is used.

II. Personal Data is Processed in the SimpleLegal Platform:

Limited Personal Data is processed by the SimpleLegal platform. This Personal Data is processed in accordance with GDPR Article 6 that describes the requirements for lawful processing of Personal Data.

Additionally, the vendors of SimpleLegal customers (typically law firms) will submit data and documents that include Personal Data of their employees and contractors (typically lawyers and paralegals).

SimpleLegal collects the following Personal Data:

Users	• First Name • Last Name • Business Email Address • IP address of the user when accessing the platform
Vendors	• First Name • Last Name • Classification

SimpleLegal does not collect the following high-risk or "special category" Personal Data of EU persons as defined in Article 9 of the GDPR:

- Race and Ethnicity
- Political Opinions
- Religious or Philosophical Beliefs
- Trade Union Membership
- Genetic or Biometric Data used to uniquely identify a natural person
- Personal Health Information
- Sexual Orientation
- Government-issued Identification Numbers
- Personal Financial Information

In the future, SimpleLegal, as the Data Processor, may be directed by the Customer, as the Data Controller, to request Race, Gender, and Ethnicity information about legal vendor employees in order to support diversity goals. Currently, SimpleLegal does not collect that information about EU persons.

III. Protection of Personal Data

Article 32 of the GDPR, requires both controllers and processors to implement "appropriate technical and organizational measures to ensure a level of security appropriate to the risk".

SimpleLegal is committed to the security and confidentiality of Customer Data. SimpleLegal employs technical and operational controls to protect Personal Data. All Personal Data are encrypted at-rest and in-transit. SimpleLegal has instituted a Business Continuity and Disaster Recovery program to ensure resiliency of the systems that process Personal Data. We conduct a third-party SOC 1 Type 2 audit annually to confirm compliance with industry standard security controls. In addition, SimpleLegal conducts third-party penetration tests to confirm the efficacy of our technical controls. SimpleLegal hosts data on the Amazon Web Services (AWS) infrastructure platform that maintains world-class security controls.

IV. Transfers of Data

Collecting Personal Data

Personal Data is collected from Customer Users in the SimpleLegal platform when the Customer creates a User. The User's first name, last name, and email address is entered by the Customer. When the User logs in to the SimpleLegal platform, the IP address of the User is captured and stored in the platform. These data elements are available to the Customer's SimpleLegal administrator user for review.

Personal Data is collected from the Customer's legal vendors when the legal vendor uploads a file containing the first name and last name of the individuals providing the legal service. This Personal Data is contained in the legal bill.

Storing Personal Data

Personal Data are stored in the SimpleLegal platform either in the US or the EU based on the Customer's requirement during the initial implementation.

Transfers of Personal Data

A Customer may access the web application from another country outside of the country where the Personal Data is stored.

Data Retention

Data is retained for up to 8 years to comply with Customer legal and contractual obligations. We may extend that period of data retention. If a Customer is no longer a SimpleLegal customer, SimpleLegal will retain a backup of the Personal Data for at least as long as contractually obligated, and in accordance with our data retention policies.

Third-Party Access to Personal Data

Your law firms and legal vendors will provide and have access to some of the Personal Data through the SimpleLegal platform. That shared access is one of the benefits of SimpleLegal.

V. Data Subject Consent

Article 6 of the GDPR describes the conditions for lawfully processing Personal Data. As it relates to Personal Data processed in the SimpleLegal platform, Customers will likely have the lawful ability to process Personal Data as the result of an employment agreement, a vendor contract, or through a legal obligation. SimpleLegal Customers typically do not need to collect a separate consent from each Data Subject in order to process Personal Data on the SimpleLegal platform. Similarly, SimpleLegal customers are not required to obtain consent to transfer Personal Data outside the EU, because SimpleLegal can commit to providing a level of protection for the data that is acceptable under EU law.

VI. Data Retention and the Right to be Forgotten

Article 17 of the GDPR describes the right to erasure, commonly known as the "right to be forgotten". The Article also includes exceptions to that right. Tax, audit, and record keeping legal requirements permit the Customer to retain Personal Data.