Smart Scribe JotPsych

Authored: July 8, 2024
Updated: July 8, 2024

Disclaimer: This document is intended as guidance, not a legal promise. It was not prepared by lawyers or technologists, and does not constitute a promise or guarantee of any kind.

SmartScribe Corp. generates notes using OpenAI and AnthropicAI, which are CCPA, GDPR, and SOC 2 compliant AI providers.

What is CCPA?

The California Consumer Privacy Act (CCPA) is a state statute intended to enhance privacy rights and consumer protection for residents of California, USA. Enacted in 2018, the CCPA gives California residents more control over the personal information that businesses collect about them.

Key Elements of CCPA:

1. **Right to Know**: Consumers have the right to know what personal information is being collected, how it is being used, and whether it is being sold or disclosed.
2. **Right to Delete**: Consumers can request the deletion of their personal information held by businesses, subject to certain exceptions.
3. **Right to Opt-Out**: Consumers have the right to opt out of the sale of their personal information to third parties.
4. **Right to Non-Discrimination**: Consumers are protected from discrimination for exercising their rights under the CCPA.

Importance of CCPA:

- **Consumer Empowerment**: Enhances consumer control over personal data.
- **Transparency**: Increases business transparency in data handling practices.
- **Data Protection**: Strengthens data protection measures for California residents.

To learn more about OpenAI's CCPA compliance, click here.
To learn more about Anthropics's CCPA compliance, click here.

What is GDPR?

The General Data Protection Regulation (GDPR) is a comprehensive data protection law implemented in the European Union (EU) in 2018. It aims to give individuals control over their personal data and to simplify the regulatory environment for international business by unifying data protection regulations within the EU.

Key Elements of GDPR:

1. **Lawfulness, Fairness, and Transparency**: Personal data must be processed lawfully, fairly, and transparently.
2. **Purpose Limitation**: Data should be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.
3. **Data Minimization**: Data collection should be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
4. **Accuracy**: Personal data must be accurate and kept up to date.
5. **Storage Limitation**: Data should be kept in a form which permits identification of data subjects for no longer than necessary.
6. **Integrity and Confidentiality**: Data must be processed in a manner that ensures appropriate security.

Importance of GDPR:

- **Data Protection**: Enhances the protection of personal data for individuals within the EU.
- **Unified Regulation**: Provides a single, harmonized data protection law across the EU.
- **Consumer Rights**: Grants individuals greater rights over their personal data.

To learn more about OpenAI's GDPR compliance, click here.

To learn more about Anthropic's GDPR compliance, click here.

What is SOC 2?

SOC 2 (Service Organization Control 2) is a framework for managing customer data based on five "trust service principles"—security, availability, processing integrity, confidentiality, and privacy. Compliance with SOC 2 is essential for any organization that handles customer data, ensuring that systems are designed to keep sensitive information secure. SOC 2 compliance is evaluated through two types of reports:

SOC 2 Type 1

- **Definition**: SOC 2 Type 1 reports evaluate the design of security processes and controls at a specific point in time. It assesses whether the system and organizational controls are suitably designed to meet the relevant trust service principles as of a specific date.
- **Focus**: The focus is on the design and implementation of the controls, providing a snapshot of the organization's control environment at the time of the audit.
- **Purpose**: This type of report is typically used by organizations to demonstrate that they have the necessary controls in place to protect customer data, even though the effectiveness of these controls over time is not assessed.

SOC 2 Type 2

- **Definition**: SOC 2 Type 2 reports evaluate the operational effectiveness of the security processes and controls over a period of time, usually a minimum of six months. It assesses not only the design of the controls but also their consistent and effective operation.
- **Focus**: The focus is on the ongoing effectiveness of the controls in place, providing a historical perspective of how well the organization has adhered to its control processes.
- **Purpose**: This type of report is more comprehensive and is used to provide assurance to customers that the organization's controls are not only properly designed but also operating effectively over time to protect customer data.

To learn more about OpenAI's SOC-2 compliance, click here.

To learn more about Anthropic's SOC-2 compliance, click here.