

GDPR, HIPAA, and CCPA

GDPR, HIPAA, and CCPA are regulatory frameworks designed to protect data privacy and ensure compliance across various industries. Here's a brief overview of each:

1. GDPR (General Data Protection Regulation)

- **Region:** European Union (EU)
- **Purpose:** Protects personal data of individuals within the EU and governs how organizations worldwide handle this data.
- **Key Principles:**
 - Lawfulness, fairness, and transparency.
 - Purpose limitation (data collected for specific purposes).
 - Data minimization (only what is necessary).
 - Accuracy and accountability.
 - Rights of individuals (e.g., access, rectification, erasure).
- **Applicability:** Any organization processing the personal data of EU residents, regardless of its location.

2. HIPAA (Health Insurance Portability and Accountability Act)

- **Region:** United States
- **Purpose:** Regulates the protection of sensitive patient health information (PHI).
- **Key Principles:**
 - Ensures the confidentiality, integrity, and availability of PHI.
 - Limits the use and sharing of PHI without patient consent.
 - Establishes standards for electronic healthcare transactions.

- Requires safeguards for data security (physical, technical, and administrative).
- **Applicability:** Healthcare providers, health plans, and any entity processing PHI.

3. CCPA (California Consumer Privacy Act)

- **Region:** California, United States
- **Purpose:** Gives California residents greater control over their personal data and ensures transparency from businesses collecting it.
- **Key Principles:**
 - Right to know what data is collected and why.
 - Right to delete personal data.
 - Right to opt-out of the sale of personal data.
 - Right to non-discrimination for exercising these rights.
- **Applicability:** Businesses meeting specific thresholds, such as annual gross revenues over \$25 million or handling data of over 50,000 California residents.