**GDPR Overview**

The **General Data Protection Regulation (GDPR)** is a comprehensive data privacy law enacted by the European Union (EU). It applies to any organization handling the personal data of EU citizens, regardless of the organization’s location.

**Key Principles of GDPR**

1. **Lawfulness, Fairness, and Transparency**: Organizations must process personal data lawfully and transparently.
2. **Purpose Limitation**: Data must be collected for specific, legitimate purposes.
3. **Data Minimization**: Only data necessary for the intended purpose should be processed.
4. **Accuracy**: Personal data must be accurate and kept up-to-date.
5. **Storage Limitation**: Data should not be retained longer than necessary.
6. **Integrity and Confidentiality**: Data must be secured against unauthorized access, loss, or damage.
7. **Accountability**: Organizations must be able to demonstrate compliance with GDPR.

**Rights of Individuals**

* **Right to Access**: Individuals can request access to their data.
* **Right to Rectification**: Incorrect data must be corrected.
* **Right to Erasure**: Individuals can request their data be deleted ("right to be forgotten").
* **Right to Data Portability**: Data can be transferred to another service.
* **Right to Object**: Individuals can object to certain types of processing, such as marketing.

**California Regulations for Data Privacy (CCPA and CPRA)**

**California Consumer Privacy Act (CCPA)**

The **CCPA** is a state law designed to protect the privacy of California residents. It grants consumers rights over their personal information collected by businesses.

**Key Rights Under CCPA**

1. **Right to Know**: Consumers can request details on what data is collected, its purpose, and with whom it is shared.
2. **Right to Delete**: Consumers can request the deletion of their personal information.
3. **Right to Opt-Out**: Consumers can opt out of the sale of their personal data.
4. **Right to Non-Discrimination**: Consumers cannot be discriminated against for exercising their rights.

**Who Must Comply?**

Businesses that meet any of the following criteria:

* Annual gross revenue exceeding $25 million.
* Collects personal data of 50,000+ consumers, households, or devices.
* Earns more than 50% of revenue from selling personal information.

**California Privacy Rights Act (CPRA)**

Effective from January 2023, **CPRA** amends and enhances CCPA. It introduces additional protections:

1. **Expanded Data Rights**: Includes the right to correct inaccurate personal data.
2. **Sensitive Personal Information**: Special rules for sensitive data like biometric or financial information.
3. **Data Minimization**: Businesses must limit data collection to what is necessary.
4. **Creation of CPPA**: Establishes the California Privacy Protection Agency (CPPA) for enforcement.

**Banking Industry Data Privacy Regulations**

**Key Compliance Requirements Under GDPR and CCPA for Banks**

1. **Data Transparency**: Banks must inform customers about what personal data is collected, why, and how it is used.
2. **Secure Transactions**: Financial information, such as account numbers and payment details, must be encrypted and protected.
3. **Consent**: Banks must obtain explicit consent before processing sensitive data under GDPR.
4. **Access and Correction**: Customers can request access to their data and correction of inaccuracies.
5. **Data Breach Notification**:
   * GDPR: Notify the regulator within 72 hours of a breach.
   * CCPA: Notify affected individuals and potentially the California Attorney General in case of breaches involving more than 500 California residents.

**How Banks Achieve Compliance**

1. **Data Mapping**: Identifying and classifying personal data processed by the bank.
2. **Secure Storage and Access Controls**: Implementing strong encryption and role-based access for sensitive data.
3. **Privacy Policies**: Publishing transparent and detailed privacy notices for customers.
4. **Third-Party Vendor Management**: Ensuring vendors handling customer data comply with GDPR/CCPA.
5. **Audits and Training**: Regular compliance audits and employee training on data privacy regulations.

**Penalties for Non-Compliance**

* **GDPR**: Fines up to €20 million or 4% of annual global turnover, whichever is higher.
* **CCPA/CPRA**: Fines of $2,500 per violation or $7,500 for intentional violations.

Both **GDPR** and **California's CCPA/CPRA** aim to protect individual privacy, though GDPR is more global, and CCPA/CPRA focuses on California residents. For banks, adherence to these regulations ensures trust, compliance, and protection against costly penalties.