SALT

General Data Protection Regulation (GDPR): Protecting Personal Data (Continued)

The GDPR regulates organizations that handle the personal data of EU residents, ensuring user privacy is safeguarded. It stresses the importance of data minimization, compelling organizations to restrict their collection and processing of personal information to what is strictly necessary. GDPR provides individuals with rights to access, correct, and delete their personal data while mandating that organizations adopt security measures by design and default. Failure to comply can lead to hefty fines and harm an organization's reputation, underscoring the critical need for GDPR compliance among businesses operating within the EU.

- Data Minimization:
  - Limiting the collection of personal data to what is necessary.
  - Deleting unnecessary personal data.
  - Anonymizing or pseudonymizing personal data when possible.
- Data Subject Rights:
  - Right to access personal data.
  - Right to rectify inaccurate personal data.
  - Right to erase personal data ("right to be forgotten").
- Security by Design and Default:
  - Implementing appropriate technical and organizational measures to protect personal data.
  - Ensuring that data protection is built into the design of systems and processes.
  - Implementing default settings that protect personal data.

Why It Matters: GDPR compliance is crucial for protecting the personal data of EU residents and maintaining their trust. Non-compliance can result in substantial fines, legal action, and damage to an organization's reputation, especially for businesses operating in or with EU residents.

API Security Requirements:

- **Data Minimization:** APIs must limit data collection to what is necessary for processing.
- **Access Controls:** Enforce token-based authentication and encryption.

Relevant Sections Referencing APIs:

- **Article 25:** APIs must follow security-by-design principles to protect user data.

How Salt Security Helps: Salt Security aids GDPR compliance by providing API discovery to identify APIs processing personal data, vulnerability assessments to detect potential security flaws, and threat protection to prevent data breaches. Salt Security's data security capabilities allow you to view personal data in motion through APIs, giving you greater control over how that data is handled. Learn more about API Security and Compliance in our **White-paper.**