Data Security & GDPR Compliance Overview

Company Information

Exported on 05/17/2023

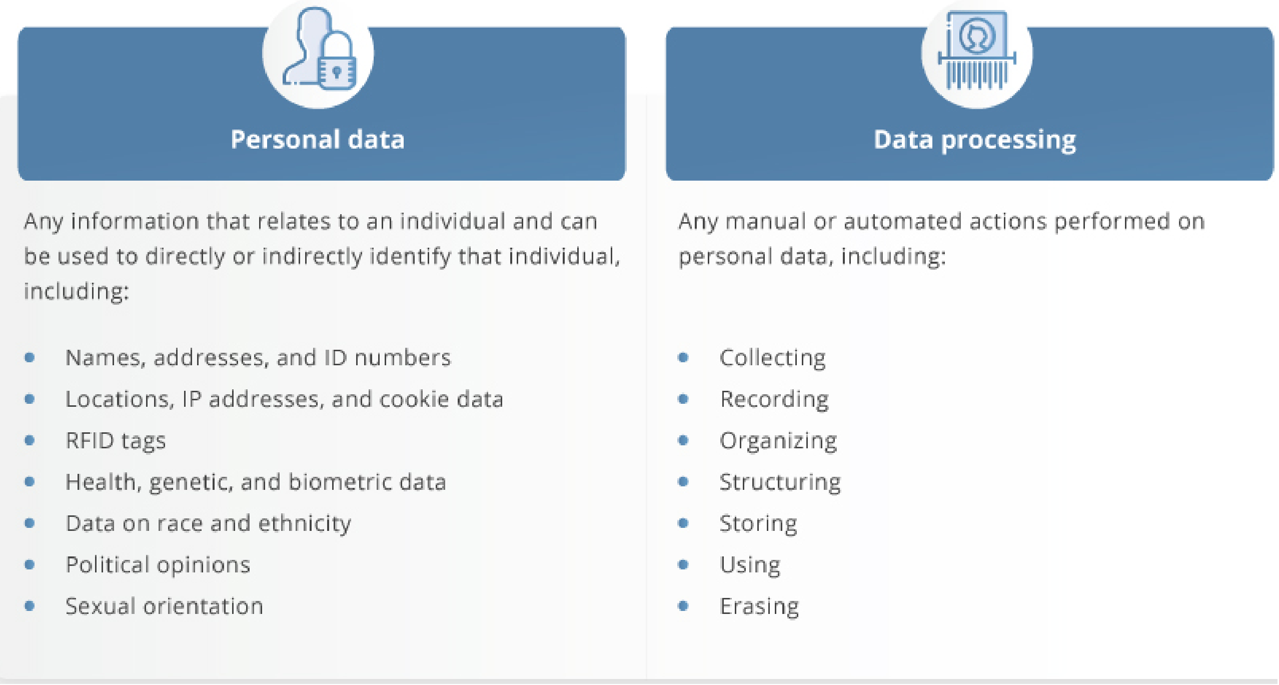
Data Security & GDPR Compliance

GDPR Compliance

The European Union's General Data Protection Regulation (GDPR) protects European Union (EU) individuals' fundamental right to privacy and the protection of personal data. The GDPR includes robust requirements that raise and harmonize standards for data protection, security, and compliance.

What is the GDPR?

The **General Data Protection Regulation** is a data privacy and security regulation adopted by the European Union (EU). It imposes obligations on all organizations that collect and process personal data of EU residents, even if these organizations operate outside the EU.



Personal data

Any information that relates to an individual and can be used to directly or indirectly identify that individual, including:

- Names, addresses, and ID numbers
- Locations, IP addresses, and cookie data
- RFID tags
- Health, genetic, and biometric data
- Data on race and ethnicity
- Political opinions
- Sexual orientation

Data processing

Any manual or automated actions performed on personal data, including:

- Collecting
- Recording
- Organizing
- Structuring
- Storing
- Using
- Erasing

Fell Tech steps to ensure full GDPR compliance and security for user data;

- Data storage within EU Region to comply with GDPR.
- Services used for user management is GDPR compliant by nature
  - AWS Cognito
  - AWS DynamoDB
  - AWS S3
- Right to be forgotten (RTBF) information website with actionable steps for user to remove all user data.
- When data is stored for statistics and metrics, data relation to specific users deleted after 30 days.
- User data for deleted users is removed in backups.
- Physical data encryption at rest, meaning that data on end devices spread throughout the world is always encrypted.

Data storage by region

2 Major data regions;

- EU
  - Data storage within EU/EØS Region to comply with GDPR.
- USA
  - Data storage physically in USA

Siloed approach for customers with specific requirements such as governmental, where a separate isolated user pool is set up. Individual country separation possible.

Company data storage and backup

- AWS Routines for storage and backup
  - Databases dumped to separate S3 storage.
  - PITR (Point in time Recovery) for all storage according to the RTO (Recovery Time Objective)
  - Code stored in Gitlab where users are authenticated to only have access to the projects they need to work.
- External backup service
  - In addition to the single-service backup of code repositories, all code, infrastructure setup and data is stored to a second source in Azure Blob Storage - Cool storage.

IT-security and security

- Compliant multi cloud environment using AWS Control Tower https://aws.amazon.com/controltower/
  - Engineer access is secured using AWS SSO with 2FA
  - Account management and governance following best practices
  - Detective guardrails to detect when policies are broken
  - Separate security accounts for auditing and cloud action logging
  - Services are split into accounts and environments to reduce blast radius for technical problems and security incidents
- Cloud is architected using the well-known AWS well-architected framework with following best practices in the security pillar
- No root users access, only in emergency scenarios (glass-break procedures)
- Ultra-specific permission schemes for production and engineering resources with access to servers

Device security / resistance to hacking

Base layer security for all IoT Devices

- ***Machine Learning Anomaly Detection*** continuously scans all running IoT devices for unregulated behavior. (e.g., the number of listening TCP/IP ports on your devices or list of IPs the device is communicating with) and the cloud (e.g., authorization failure count).
  - Audit monitors your device-related policies, certificates, and other resources to ensure that the proper security configuration is in place.

Device security

- Local radio interfaces inherently secure because all wireless communication is encrypted with minimum AES128 encryption.
- Client certificates must be registered with AWS IoT before a client can communicate with AWS IoT. This certificate is generated per device, and hard-coded into the device during production.
- There are no “open” communication links between local peripherals wires and wireless (Zigbee, Bluetooth, WiMEA, Modbus) and cloud. Only pre-defined API-layers available if a certificate was breached.
- Low level OS implementation based on FreeRTOS which does not contain additional services for potential security issues such as RDP.
- All traffic to and from cloud is encrypted using Transport Layer Security (TLS).

Well-Architected Framework

Fell Tech commits to follow the five pillars of the Well-Architected Framework to review and improve our cloud-based architectures and better understand the business impact of the design decisions we make. The Well-Architected Framework describes general design principles, as well as specific best practices and guidance for the five pillars of the Well-Architected Framework.

References

https://docs.aws.amazon.com/wellarchitected/latest/iot-lens/security-pillar.html