Article
Yuri Marx · Jun 8, 2020 3m read

Compliance of data solutions based on InterSystems technology with GDPR (Europe), CCPA (California) and LGPD (Brazil)

About regulations

Personal data privacy regulations have become an indispensable requirement for projects dealing with personal data. The compliance with these laws is based on 4 principles:

1. Compliance with the rights of the holder of personal data;
2. Governance of personal data assets;
3. Privacy by Design and by Default;
4. Data protection.

In case of violation in the treatment of personal data, controllers and operators of these data may suffer:

1. Fines of up to 4% of revenue or up to €20 million;
2. Shutdown of the digital service until the problem is corrected;
3. Publicity of the incident to the public.

Take Action

Administrators, developers and managers of data platforms on InterSystems technology can take the following detailed measures to help comply with personal data protection laws.

In compliance with the rights of the holder

- Create APIs using Interoperability IRIS ESB for consumption in a Portal for the end user to exercise their rights. The APIs must allow to the holder:
    - Consult the personal data that the controller keeps about the holder. Allow downloading this query in open format (JSON).
    - Allow the holder to correct personal data. Use the IRIS ESB to record changes on each system where this personal data exists.
    - Implement a consent management service for sharing and processing personal data, especially sensitive data. In the InterSystems Health services the HIPAA is enough.
    - Allow the holder to consult with whom their data has been shared.
    - Build an interoperability service (ESB) with the internal service system to receive requests from the holder.

In personal data governance

- Catalog persistent classes, productions and BI cubes that store or process personal data. Use XData for this. It is necessary to catalog whether it is personal or sensitive data, purpose of processing, technical and business responsible and for how long the data will be stored.
- Perform good data access management.

- Manage the data lifecycle by creating a procedure for disposing of data after the legal custody period.
- Monitor and audit data flows.

In privacy by design and by default

- Architect and design persistent objects or namespaces that deal with personal data with:
    - Create a DPIA (Data Protection Impact Assessment) when deals with sensitive data, high volume data, personal profile production and use of new technologies (Machine Learning);
    - Use managed key encryption to the sensitive data;
    - Use TLS and HTTPS to message channels.
    - Add DevSecOps in your DevOps initiative.
    - Create docker models with security and best practices set by default.
    - Include automated tests to security checks.

In Security Protection

- Create an efficient procedure to backup and restore data. The backup must be cryptographed;
- Work your environment in a High Availability;
- Protect your API with IRIS API Management;
- Protect your persistent objects with good authentication and authorization procedures;
- Enable logs and use ESB to log end to end the sensitive operations;
- Create Cybersecurity Guide;
- Create IT Security Guide;
- Create Data Privacy Guide.

#Databases #Encryption #InterSystems Business Solutions and Architectures #Security #Caché #Ensemble #InterSystems IRIS #InterSystems IRIS for Health

---

Source URL:https://community.intersystems.com/post/compliance-data-solutions-based-intersystems-technology-gdpr-europe-ccpa-california-and-lgpd