Implementing IoT to Comply with GDPR

Five key transition benefits to increase ease of compliance with regulation EU 2016/679

by Bryan Kissel and David Wolf

The impetus of the GDPR (General Data Protection Regulation) is to establish reasonable protection Articles for any systems that access, process or otherwise 'touch' the personal data of EU citizens. The GDPR creates a standard methodology for data protection and establishes rights for individuals whose data is used in any way for any business purpose.

Any company operating in the EU or selling products into the EU will need to comply. Here's how the Internet of Things (IoT) can help.

The Challenge of GDPR

Modern data systems including cloud environments, mobile devices, IoT and hosted services create new challenges for data security. These databases have the potential to personally identify users, storing data including national IDs, driver's license numbers, email addresses, location data (including cookies and IP addresses) and biometric data, as well as personal information such as political party affiliation, religious identity, genetic identifiers, mental/physical health information and gender. These data points are all considered protected personal data objects by the GDPR.

The GDPR builds on existing standards by establishing an expectation of consumer rights to access, correction and erasure. Where standards like ISO, FIPS, the EU MDR and HIPPA in the US establish rules for access, auditing, distribution and securing protected data, the GDPR adds a layer of accountability and visibility specifically to protect and inform the consumers whose data is used and governed by these regulatory agencies. Where HIPPA focuses on the protected data used within the medical industry, the GDPR applies these principles to all industries who use identifiable data. Maturing compliance across the enterprise requires both adoption of leading practices for security and hardening of existing strategies to meet new regulatory challenges. It also requires enhanced security capabilities built on existing processes and infrastructure to increase ease of adoption.

Basic GDPR Requirements

GDPR obligations can be difficult to navigate and establishing a reasonable compliance roadmap is essential to satisfying the GDPR.

Traditionally, an assessment of an organization's data privacy and security practices would establish a baseline risk model and the processes needed to mitigate those risks, most importantly ***identifying*** and ***classifying*** personal data that qualifies as 'protected data subjects.'

To satisfy the GDPR, companies must understand:

- Where the enterprise stores personal data objects
- What applications and services leverage that data
- Which users access that data

The GDPR requires data custodians to look *beyond* IT and in to all lines of business that may be exposed to or have access to personal data objects of EU citizens.

Once identified, systems carrying this data must satisfy four primary consumer rights objectives:

1. Explicit, conditional and on-going consent from data subjects
2. Data subject right to access their related information (including visibility to use and access of that data)
3. Data subject right to erasure of said data
4. Data subject right to objection and rectification of incorrect data

These objectives create a layer of transparency previously not required of the enterprise. Cloud environments, applications, learning platforms, analytics platforms, databases and file systems are all subject to GDPR standards. Industry trends in data security and risk mitigation also guide the Chief Security Officer in securing data in-flight.

Email, IM, screen share and other forms of data transmission are also GDPR regulated, meaning data in the enterprise email platform, if housing protected data, must also comply with the security policies established to protect personally identifiable data. More than 90% of targeted cyber-attacks start with email. Prevent email attacks that can lead to personal EU data being stolen, damaged, or exposed by

encrypting emails.

Addressing GDPR with IoT

An IoT platform like ThingWorx™ substantially accelerates satisfaction of these objectives by leveraging a highly extensible and flexible framework. ThingWorx can leverage partners (ie: PingFederate for SSO support) and internal development teams to create adaptive solutions that meet business needs ***and*** satisfy the GDPR.

There are technical requirements of the GDPR that will affect a majority of the enterprise. For example, the articles of the GDPR explicitly require data custodians to make reasonable efforts to encrypt and secure data, which includes the replacement or removal of applications and tools that are considered 'end of life' and no longer supported by the original enterprise manufacturer.

The most important aspect of the GDPR is its global reach. Any organization doing business in the EU is subject to the GDPR. Establishing leading practices to identify personal data and reduce risks is the ***core principle*** of the GDPR. An IoT platform like ThingWorx, with advanced functionality, support options, scalable monitoring and modern data protection services at its core, increases ease of compliance and speed of adoption.

Five Ways ThingWorx Enables GDPR Compliance

Built-In Security Features
The ThingWorx platform has a robust information security suite that is highly customizable per business needs. Development of APIs and plugins to provide on-demand analytics tools is a cornerstone of the ThingWorx platform. SSO and Two Factor Authentication (2-FA) are important built-in features.

ThingWorx adds a host of advanced security capabilities that can further enhance security posture. Support for SQL and Cassandra, 'Internal Secret' protocols leveraging AES128 encryption, and Tomcat 8.5 support ensures the hosting mechanism has never been more secure. Intelligent logging strategies narrow the scope of log collection and streamline the review and audit process.

Discovery, Management and Provisioning of Personal Data
A significant challenge of the GDPR is the identification and classification of personal data objects. This new requirement establishes the need to perform a personal data audit to determine any preexisting compliance risks that exist from unclassified or otherwise unidentified personal data.

ThingWorx can identify and organize personal data including age, date of birth, gender, email address, name, passport/license information, location/GPS data, criminal records, biometric data, photo, address, IP address and other personally identifying information, providing a snapshot of data related to specific data subjects.

This snapshot allows a detailed view of all personal data attached to any given profile, and allows those persons to review, confirm or request redaction/erasure of data elements.

Scalable Monitoring Solutions
The ThingWorx platform leverages proprietary identity asset management strategies that create a real-time access and activity auditing trail for all user activities within ThingWorx. Visibility to who is accessing data and what data is accessed, and the ability to create benchmarks for acceptable use models is built in to ThingWorx. Data integrity is further ensured by monitoring user permissions, accessibility windows and reporting anomalous activities to the ThingWorx administrator.

End-To-End Data Protection
The ThingWorx solution leverages Transport Layer Security (TLS) encryption standards for data both at rest and in flight, ensuring that personal data, and all data objects used in the ThingWorx solution, are appropriately obfuscated from unauthorized viewers.

Industry-Leading Development Flexibility
Innovation is a core principle of the ThingWorx platform, including the ability to quickly create intelligent, agile response plans to outstanding business needs. Robust platform features combined with deep expertise and a proven methodology help companies identify risk areas managed by the GDPR and streamline the rectification process to reduce time to compliance in any size enterprise.

LINKS AND SOURCES:

The GDPR and all Articles: https://gdprinfo.eu/
Final Ver of Regulations of Enforcement: http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf
Interdisciplinary Centre for Law and ICT: http://blogs.lse.ac.uk/mediapolicyproject/2014/04/11/data-portability-series-at-the-crossroads-of-protection-and-competition-policy/

Originally published on February 28th, 2018

What's your view? Add your question or comment

About the Authors

Bryan Kissel

bryan.kissel@kalypso.com

Bryan is a manager in Kalypso's digital practice. He is based out of Dallas and can usually be found programming synthesizers or cataloging compliance gaps to bring up again later.

David Wolf

david.wolf@kalypso.com

David is a Senior Manager and Biomedical Auditor with over 25 years of experience in the life sciences industry. He's designed 3D assemblies, manufacturing toolpaths, submitted patents and personally worked with doctors all over the world to validate and release several product lines.