

EXECUTIVE BRIEF

Retailers: Turn GDPR compliance into a competitive advantage

Impacts of the new EU data privacy law on retail



GDPR is good for business



Improve information governance



Deliver more personalization



Build consumer trust

The General Data Protection Regulation (GDPR) is the new European Union legislation to modernize the laws that address the handling of personal data. It applies to any retailers who collect and store the personal data of EU citizens, even if they don't have a formal presence in the EU zone. In addition to financial penalties for non-compliance, retailers risk losing consumer trust and damaging brand reputation if personal data isn't handled properly.

The GDPR is a wake-up call for issues of data privacy, security breaches and information governance. Retailers have collected consumer preferences and purchase histories for years without explicit permission or without disclosing details on how the data will be used. Hackers regularly target retailers to extract this wealth of consumer and financial information. For example, in 2017, Saks Fifth Avenue, Brooks Brothers, Whole Foods, Forever 21 and eBay dealt with data breaches, and other retailers are still reeling from the continued impact of previous breaches. To earn customer trust and loyalty, retailers must have a unified approach to information governance.

Follow the path to readiness

View the [infographic](#) to learn 7 easy steps to GDPR readiness.

Join the conversation

[GDPR. Forget Bitcoin, data is the new currency of Retail »](#)

[The GDPR and Digital Marketing »](#)

[Kickstart your GDPR program »](#)

Learn more

[Start a GDPR action plan »](#)

[Identify and remediate breaches »](#)

Download

[What does GDPR Mean for B2B Organizations? \(White paper\) »](#)

The GDPR opportunity: Data-driven customer focus

Retailers have long talked about becoming more data driven and leveraging that data to develop new products and services, while increasing business efficiencies. The GDPR ushers in a new data-driven generation. The regulation provides an opportunity to use data to build trust and cement customer relationships through personalization and superior omnichannel experience. With complete control and visibility of data consented by consumers, retailers can apply greater analytics to deliver enhanced insight and personalization that leads to superior customer experience.

However, the challenges of compliance should not be underestimated. Retailers need to address all the personal data they have, and understand how it's being used and by whom. OpenText facilitates this process with an Enterprise Information Management (EIM) platform that ensure businesses have total control of all the data and content within their organizations.

Follow these steps to locate and protect data:

1. **Locate all the personal information** in the organization with data discovery, including: identifying which processes use the data; documenting the consent; describing if and how personal data moved to third parties and cross border. This will identify information that is scattered across multiple databases including eCommerce and store operations, customer service and loyalty programs.
2. **Manage personal information** for data minimization by classifying it and ensuring processes and systems follow data protection by design and default principles. This requires creating defensible records retention and disposition, and creating unified repositories. Remove internal silos that separate online and store operations that impede a seamless omnichannel experience. When new commerce and customer service technologies are implemented, decommission any legacy systems while retaining access to critical customer data.
3. **Protect and secure personal information** throughout its lifecycle. Retailers must be able to quickly identify and remediate if a data breach occurs, and conduct analyses of events and breaches that have occurred.