The GDPR and EU Data Protection—Challenges Ahead for Retailers

Retailers have access to a huge amount of consumer data thanks to digital technology, and consequently are exposed to the risk of breaching data protection regulations. Companies operating in the European Union (EU) need to comply with EU legislation on data protection. This report provides an overview of the latest EU legislation which will come into force in May 2018—the General Data Protection Regulation (GDPR)—and its implications for retailers, and suggest how retailers can prepare for the new regime. The report touches on these main points:

1) Companies targeting consumers based in the EU are currently subject to the EU Data Protection Directive that will be replaced by the more restrictive GDPR in 2018.

2) The GDPR introduces significant changes in the level of data protection. For example, the new regulation makes it easier for individuals to bring claims against companies processing data.

3) Retailers targeting EU consumers will need to prepare to comply with the new regulation, even if they are based outside the EU—for example by training staff on compliance and by setting up clear accountability procedures.

Deborah Weinswig
Managing Director,
Fung Global Retail & Technology
deborahweinswig@fung1937.com
US: 917.655.6790
HK: 852.6119.1779
CN: 86.186.1420.3016

Introduction

Retailers have access to a huge amount of consumer data thanks to the application of digital technology to their operations.

Retailers have access to a huge amount of consumer data thanks to the application of digital technology to their operations. For example, shoppers visiting online stores leave a digital footprint of their shopping behavior, and even those going to brick-and-mortar stores leave traces when retailers use technologies such as radio frequency identification (RFID) or near field communication (NFC) to engage with shoppers.

This access to valuable consumer data is a great opportunity for retailers to better understand their customer base and to provide better service. However, the flipside of this is the responsibility that comes with the handling of personal data.

In particular, retailers that deal with consumers based in the EU need to consider the implications of the EU provisions that regulate data protection. The matter is currently regulated by the 1995 EU Data Protection Directive, but a new regulation—the General Data Protection Regulation (GDPR)—that goes into effect on May 25, 2018, will introduce more stringent provisions for organizations processing consumer data.

This report provides an overview of the new legislation, its key changes compared to the current directive and the implications of the new data protection regulation for the retail industry, as well as shows how retailers can prepare and respond to the more stringent regulatory provisions.

The Data Protection Directive–Background of the Current Legislation

In the EU, privacy and data protection are currently regulated by the Data Protection Directive, adopted in 1995.

In the EU, privacy and data protection are currently regulated by the Data Protection Directive (DPD), adopted in 1995. The Directive states that data processing is only lawful if the data subject—the individual whose data is collected—has unambiguously given consent. The EU Directive was implemented by national parliaments of the member states. In the UK, the DPD was implemented through the Data Protection Act 1998 (DPA).

For clarity, we briefly consider how retailers are subjected to the DPA's provisions.

The DPA regulates the processing of personal data by two stakeholders, which are identified as:

- **Data controller:** The person (physical or legal) who determines the purpose for processing personal data and the way data are processed.
- **Data processor:** The person who processes the data on behalf of the data controller.

Data controllers and data processors can be companies processing their own customers' data. In most cases, data controllers and processors are part of the same organization—the two functions are often assigned to different departments within the same company. The data controller can be a retailer collecting customers' data using RFID technology. The collected data could be processed by the retailer itself or by a third-party company to which the retailer has subcontracted the function.

Under the DPA, data controllers handle personal data according to a series of key principles. For example, they must process data fairly and lawfully,

Deborah Weinswig, Managing Director, Fung Global Retail & Technology
deborahweinswig@fung1937.com US: 917.655.6790 HK: 852.6119.1779 CN: 86.186.1420.3016

for specified purposes, and they are obliged to keep the data secure and only for the necessary period, and to not transfer the information outside the EU without adequate protection.

The DPA gives the entire responsibility for compliance to the controller, who must ensure that the processor complies with the principles. Failure to comply can result in penalties and even criminal prosecution for the controller.

The GDPR introduces a stricter data protection compliance regime and puts direct obligations on processors for the first time.

How the Use of RFID is Regulated by the EU

RFID devices are used by retailers for customer engagement. The European Commission released the EU Regulatory Technical Standards in 2014 to help companies using RFID comply with EU data protection rules laid out in the 1995 Data Protection Directive.

According to the Regulatory Technical Standards, retailers should:

1. Give consumers clear and simple information on what type of data will be collected and how their data will be used and for what purpose.
2. Provide clear labeling to identify the devices that collect the data.
3. Conduct privacy and data protection impact assessments before using RFID devices.

This is the label used to identify RFID devices that must be displayed in stores that use such devices, according to the EU Regulatory Technical Standards.
Source: Europa.eu

Deborah Weinswig, Managing Director, Fung Global Retail & Technology
deborahweinswig@fung1937.com US: 917.655.6790 HK: 852.6119.1779 CN: 86.186.1420.3016

Introducing the General Data Protection Regulation

The new GDPR, adopted in 2016, will replace the EU Data Protection Directive (and the related national acts such as the UK DPA) when it comes into force on May 25, 2018. The GDPR introduces a stricter data protection compliance regime and puts direct obligations on processors for the first time. Moreover, the Directive enables consumers to enforce their rights against firms processing data and facilitates the application of tougher sanctions on noncompliant companies.

Businesses targeting European consumers will need to prepare to comply with the new regulation, even if they are based outside the EU.

Businesses targeting European consumers will need to prepare to comply with the new regulation, even if they are based outside the EU, as the regulation applies to the treatment of data belonging to EU subjects, regardless of where the data controller and processor are based. Unlike the current DPD, the GDPR will be enforced directly in the EU member states, without the need for legislative intervention by national parliaments. In this way, the GDPR will limit the possibility of diverging interpretations of the regulation in different jurisdictions.

Brexit will not make British-based firms exempt from the GDPR, given that it will be enforced prior to the date when negotiations between the UK and the EU end (the most optimistic deadline is two years from March 2017, when Article 50 was triggered). Even after the UK exits the EU, British companies targeting EU consumers will still need to comply, given the extraterritoriality of the GDPR.

The text of the GDPR explicitly states its application to the processing of personal data of data subjects related to the offering of goods and services or the monitoring of their behavior. Moreover, the text mentions that online identifiers such as RFID tags can be used to profile a person, thereby creating the case for the application of data protection principles to the use of RFID technology.

Source: iStockphoto

The GDPR does not significantly change the data protection principles as listed in the previous Directive. According to the GDPR, personal data must be processed lawfully, fairly and transparently; collected accurately and safely; and stored with a specific purpose in mind. The controller is responsible for and must be able to demonstrate compliance with the data protection principles. The GDPR also requires processors to comply with certain obligations, such as maintaining adequate documentation, and will be directly liable to sanctions if they fail to meet these criteria.

However, the GDPR presents significant changes in the level of data protection and is a big step up from the provisions of the current DPD. Figure 1 summarizes the key changes and possible implications for retailers using RFID.

Deborah Weinswig, Managing Director, Fung Global Retail & Technology
deborahweinswig@fung1937.com US: 917.655.6790 HK: 852.6119.1779 CN: 86.186.1420.3016

Figure 1. GDPR: Key Changes and Potential Impact on Retailers Using RFID

Change	Meaning	Potential Impact on Retailers
Wider Territorial Scope	The GDPR applies to companies based outside the EU that collect data inside the EU.	The GDPR applies to all retailers with operations in the EU.
Tougher Sanctions	Sanctions for data protection breaches could be up to 4% of a company's annual worldwide turnover.	Retailers with international operations can incur much higher sanctions, calculated as a percentage of global turnover, even if a breach occurs within only a single division of the company.
Broader Definition of Personal Data	The GDPR expands the definition of personal data to include information such as identification numbers, location data, online identifiers and other factors that may identify a natural person. Online identifiers are listed as IP addresses, cookies and RFID tags.	Data protection regulation will apply to consumers' online identifiers collected by retailers operating online and to data collected though in-store technology such as RFID.
More Rights for Individuals	The GDPR makes it easier for individuals or groups of individuals to bring private claims against companies processing data. For instance, data subjects will be able to claim compensation for "non-material damages," will have enhanced rights such as the right to greater transparency, and additional rights, including the right to be forgotten, which requires companies to remove an individual's data from their databases if the firm has no legal ground for processing the information.	Retailers collecting data may be more likely to incur claims on data protection from individuals or groups of organized individuals.
Processors are Liable	The GDPR also regulates processors, requiring that they maintain adequate documentation, implement appropriate security standards and appoint data protection officers, among other obligations	The GDPR increases the compliance burden by making the processor liable. Given that processors and controllers can be different departments within the same company, the provision might result in duplication of tasks within an organization.
Valid Consent Harder to Obtain	Consent to have one's data collected must be fully unbundled from other terms and conditions, and can be withdrawn at any time.	The GDPR makes it harder for retailers to fall within the legal justification for the process of data gathering using RFID technology.
Data Breach Notification	The GDPR requires companies (both controllers and processors) to notify authorities and affected individuals of data breaches.	Data breaches due to cybercrime, lost or stolen devices and e-mails sent to wrong addresses are relatively common. Retailers need to adopt a coordinated approach to minimize their risk, including use of technology, breach response procedures and staff training.
Enhanced Data Subject Rights	Controllers must provide data subjects with greater transparency in communications relating to the use of personal data. Data subjects have additional rights, such as the right to object and the right to be forgotten.	Retailers will need to review their data collection procedures to ensure compliance.
Data Protection Officers (DPOs)	In some cases, the GDPR requires companies to appoint a DPO, such as when the organization processes data on a large scale.	Retailers are unlikely to be subject to this obligation, but they should conduct an assessment to determine whether or not this provision is applicable to the kind of data they use.
Accountability	Organizations need to demonstrate compliance with the GDPR's data protection principles.	Retailers will need to keep detailed records of data-processing operations.
Cross-Border Enforcement	A controller with a presence in multiple EU member states will be potentially subject to multiple countries' regulators.	Retailers carrying or processing customers' data will have to determine which authorities have jurisdictions over their activities.

Source: Europa.eu/DLAPiper.com

Deborah Weinswig, Managing Director, Fung Global Retail & Technology
deborahweinswig@fung1937.com US: 917.655.6790 HK: 852.6119.1779 CN: 86.186.1420.3016

The GDPR entails a significant increase in accountability in terms of data protection and in administrative burden for retailers processing customers' data.

How Retailers Can Prepare for the GDPR

The GDPR entails a significant increase in accountability in terms of data protection and in administrative burden for retailers processing customers' data. However, we do not think that the GDPR will put at stake retailers' abilities to take advantage of consumer data, as long as companies take action to prepare for the new regulation.

In particular, retailers should:

1. **Analyze the legal basis on which data are used:** Understand whether the use of the tracking technology falls under the provisions of the GDPR. For example, some uses of RFID can be considered as tracking product movements in-store, rather than customer behavior. In those cases, the use of RFID could be exempted from the regulation.
2. **Review strategies for data processing and recording:** Review and enhance the procedures used to track records of data-processing activities and ensure appropriate documentation is kept.
3. **Set up clear compliance accountability procedures:** Given that different divisions in an organization will have greater accountability, it is important to set precise procedures that assign clear responsibilities within the company.
4. **Train staff on data protection:** The increased accountability within different divisions of a company exposes more staff to the responsibility of compliance and requires that employees not previously involved be adequately trained.
5. **Review the use of subcontractors:** When choosing a data collector that is a third-party organization, it is important to appoint a company that can ensure compliance.
6. **Prepare for data breaches:** Set up an efficient notification system and put in place clear procedures to ensure a fast reaction to data breaches.
7. **Prepare for data subjects' claims:** Prevent claims from customers by setting up clear and explicit data consent policies, and prepare for customers to exercise their rights with procedures that ensure effective responses.
8. **Understand which regulators have jurisdiction over international operations:** It is important for retailers that operate internationally to determine which authorities have jurisdiction over data-processing activities in different countries.

Deborah Weinswig, Managing Director, Fung Global Retail & Technology
deborahweinswig@fung1937.com US: 917.655.6790 HK: 852.6119.1779 CN: 86.186.1420.3016

We believe that companies that prepare well for the GDPR will not jeopardize their ability to take advantage of the insight provided by consumer data despite the more restrictive regime that they will face.

Key Takeaways

Retailers have access to a huge amount of customer data thanks to the application of digital technology to their operations, but while this is an opportunity to better understand the customer base, the broader availability of personal data exposes companies to the risk of breaching data protection regulations.

In the EU, privacy and data protection are currently regulated by the Data Protection Directive, but the GDPR will replace the current legislation when it comes into force on May 25, 2018, and will introduce a stricter data protection compliance regime. The GDPR introduces significant changes in the level of data protection. For example, the new regulation makes it easier for individuals to bring claims against companies processing data.

Retailers targeting European consumers will need to prepare to comply with the new EU regulation, even if they are based outside the EU, for example by training staff on compliance and by setting up clear accountability procedures. We believe that companies that prepare well for the GDPR will not jeopardize their ability to take advantage of the insight provided by consumer data despite the more restrictive regime that they will face.

Deborah Weinswig, Managing Director, Fung Global Retail & Technology
deborahweinswig@fung1937.com US: 917.655.6790 HK: 852.6119.1779 CN: 86.186.1420.3016

Deborah Weinswig, CPA
Managing Director
Fung Global Retail & Technology
New York: 917.655.6790
Hong Kong: 852.6119.1779
China: 86.186.1420.3016
deborahweinswig@fung1937.com

Filippo Battaini
Research Associate

Hong Kong:
8th Floor, LiFung Tower
888 Cheung Sha Wan Road, Kowloon
Hong Kong
Tel: 852 2300 4406

London:
242-246 Marylebone Road
London, NW1 6JQ
United Kingdom
Tel: 44 (0)20 7616 8988

New York:
1359 Broadway, 18th Floor
New York, NY 10018
Tel: 646 839 7017

FungGlobalRetailTech.com