Panasonic
BUSINESS

IN-STORE INSIGHTS REPORT: HOW DATA ENHANCES THE CUSTOMER EXPERIENCE IN RETAIL

Industry-specific Research on Data Usage
incl. a GDPR Checklist

It is well-known that the retail industry is one of those most affected by GDPR due to the amount of customer data it handles. The complexity of how it gathers customer data, how it stores such data and what it does with the data has resulted in navigating a minefield to guarantee compliance. With customers also now able to govern compliance by monitoring and reporting misuse of their personal information, what should retailers be most aware of?

How data enhances the customer experience in retail is part of a white paper series targeted at providing the retail industry with information on technology that can help bricks and mortar retailers in increasingly challenging market conditions.

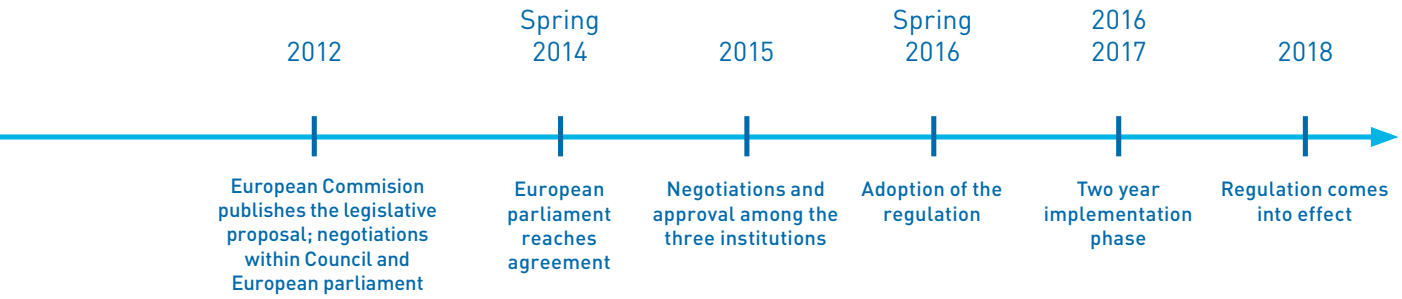
General information on the GDPR

The General Data Protection Regulation (GDPR) applies to every organisation worldwide that processes, stores or transmits personal data of EU residents, making it the first global data protection law. It considers any data as personal data that can be used to identify a person, such as someone's IP-address, passport number or a person's physical, genetic, mental, cultural or social attributes. This means there is hardly any data not covered by the GDPR.

Furthermore, the legislation requires all public authorities processing personal information, and any other organisations whose core activities require regular and systematic monitoring of data subjects on a large scale, to appoint a data protection officer (DPO). The appointment of a DPO is also mandatory if a company processes sensitive data or data relating to criminal convictions. If organisations want to collect personal data, they have to ask their customers for consent in plain language and they have to be clear about how they will use the information. On top of that, companies are not allowed to hold data for any longer than absolutely necessary and they must not change the use of the data from the purpose for which it was originally collected.

When organisations become aware of personal data breaches, they have to report it to the relevant authorities within 72 hours. Non-compliance with any requirements of the GDPR can be fined up to 4% of their annual global turnover or up €20 million, whichever is higher.

The legislation also gives consumers a number of rights. People can request information about the data an organisation stores about them and demand a company deletes all data, at any time. Customers can also demand organisations to hand over all data they have collected about them at any time.



Source: https://www.iocea.com/blog/gdpr_enforcement/

How do retailers currently collect data?

There are a number of ways retailers can collect data about their customers. One way this is done is by installing cameras in stores, so that shop owners can collect information on their **customers' gender, age and happiness**, as well as on the **routes** they take in the store. While this data tends not to be anonymised and not stored against a personal data profile, it does allow retailers to identify areas with little traffic and thus improve the layout of the store. At the same time observing customers' happiness allows conclusions to be drawn on the overall shopping experience. Another way to collect data on customers' shopping habits is through loyalty programmes. Analysing this data enables retailers to target their customers more effectively. By partnering with other businesses, companies are able to gain even deeper insights into spend patterns through data sharing. For example, by using data to identify future mums before other retailers do, a retailer is able to provide targeted offers and capture their regular spend as they transform their previous spending habits.

By providing **free Wi-Fi** and analysing users' browsing behavior, retailers can uncover what websites shoppers are visiting while travelling through certain areas of a store or shopping mall. Using apps, point-of-sale data, and security cameras, retailers can develop a greater understanding of who exactly is shopping at any time and what these consumers' shopping habits and preferences are.

How and where do customers see sharing more data will benefit them?

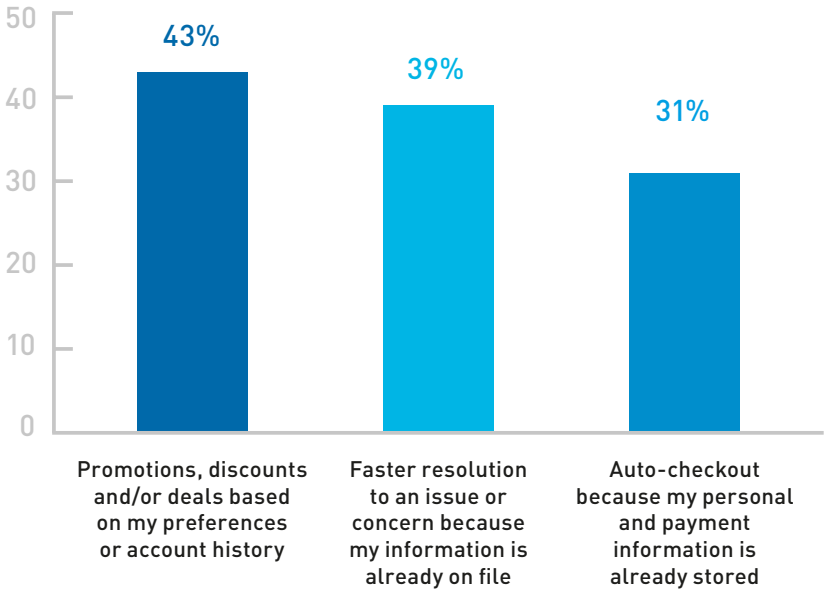
A survey conducted by Deloitte revealed that 48 percent of all consumers and 58 percent of Millennials are willing to share more data in return for a **personalised service**. According to the study, more consumers are starting to share their location and personal details to acquire better service from a store or to receive more personalised emails with recommendations.

People are also more willing to share personal data in the future if they receive **discounts** in return. PwC found that 41 percent of consumers are comfortable for retailers to monitor their shopping patterns and purchases to tailor offers specifically for them. This was mirrored by 43 percent of respondents to a YouGov study, who indicated they would share more personal data if it got them more discounts based on their preferences.

In the same YouGov study, 39 percent of respondents stated they would share more data if it helped the retailer to **resolve issues faster** because their data is already on file. Furthermore, they were willing to share payment data if it would enable them to **auto-checkout**. 49 percent of PWC survey respondents are also willing to share personal information if it enables them to **quickly find shops nearby**. The willingness to share data to get information about the closest shops is highest for 18-29 year-olds (55 percent).

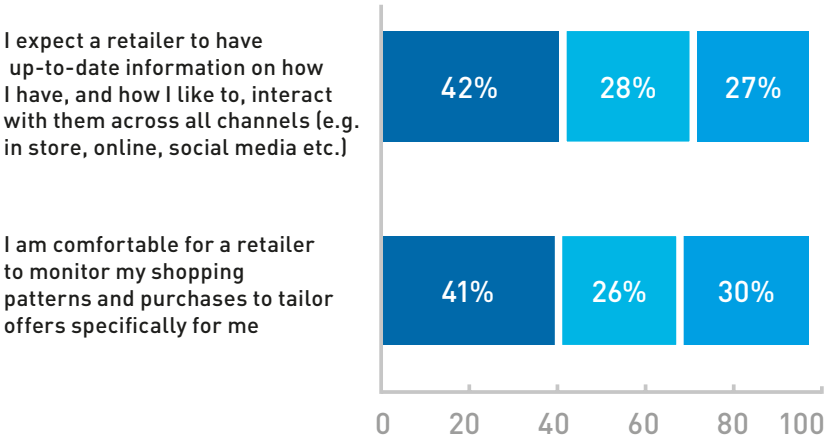
Ultimately, sharing personal information is not generally an issue for consumers. As long as the benefit is clear and the shopping experience is enhanced, there are few barriers for their data to be shared and analysed. GDPR then applies to how retailers keep such data safe and ensure it's used only with the original intention agreed by the customer.

Reasons for sharing personal data



Source: https://marketingland.com/survey-consumers-willing-share-personal-data-deals-better-customer-service-212232

In the age of increasing surveillance, the biggest concerns for consumers are around being tracked



Source: https://www.pwc.com/gx/en/retail-consumer/assets/consumer-trust-global-consumer-insights-survey.pdf (p. 7)

GDPR Top Tips for Retailers

The importance of data-sharing for successful Retailer - Customer relationships is stronger than ever. Customers expect the advantages that sharing their data can bring. The General Data Protection Regulation (GDPR) has added a layer of security and compliance to how Retailers manage this data. The following checklist has been created to provide confidence that the key areas are covered and that consistency can be achieved throughout the whole retail organisation.

Role & Responsibility of a Data Protection Officer

The data protection officer is responsible for overseeing your organisation's data protection strategy and ensuring compliance with the GDPR requirements.

1. **Appoint a GDPR lead:** Retailers need to appoint a specified Data Protection Officer. ☐
2. **Clearly define roles and lines of responsibility:** There are multiple roles for compliance ownership and liability. Examples of cross-over may be between data controllers and data processors, and security and IT departments. Refer to the ICO tool: – For data controllers – For data processors ☐
3. **Educate staff:** All staff, including shop floor workers and security teams must be aware of people's rights to request a copy of data collected of them – including images. ☐
4. **Be clear on how long data can be retained:** Align data retention periods for footage and subject access request requirements across European countries, and ensure all employees understand these. ☐
5. **Be cognisant of holding and sharing information** pertaining to third parties, and keep a record of all access requests. ☐

"Stores need to become connected, interactive environments but also take care of reducing the daily threats of having a physical presence, like Shoplifting; a threat that is increasing year-by-year in many countries. To ensure this, German data controllers have to adopt technical measures to enable them to meet these challenges under the new laws. Protecting the business with secure and reliable technologies is crucial. Fortunately, technology today is flexible enough to meet data privacy demands with masking identity and secure communications functionalities." | **Ye-Un Lee-Strasburger, Business Development Europe, Panasonic Business**

"Retailers need to use the new legislation as an opportunity to reconnect in a more specific and meaningful way with their customers. Communicating to the customer that not only 'their thoughts matter' but linking their personal needs and data is key to both enhancing their in-store experience and rewarding loyalty. As long as the reasons for having personal data are legitimate and relevant, there shouldn't be an issue in the UK." | **Gary Byrne, Retail Solutions UK, Panasonic Business**

Be aware of the age of your customer

Each member state will have its own age limit (between 13 and 16 years of age) for data information requests. Data controllers must ensure the business is aware of differing age limits in other countries.

6. **Update signage to demonstrate consent:** All signage must be clear, visible and readable. Include the purpose of security systems, the operating system used and who to contact in the event of any query. ☐

7. **Anonymity first:** Consider adopting technology that enables the business to mask images of individuals until they are officially required for evidential purpose. ☐

8. **Be confident across multiple sites:** Ensure compliance is being enforced across all European stores, that updates to signage are complete and that the responsibilities of those implementing updates are clearly set out and understood. ☐

9. **Confirm your lead data protection supervisory authority:** This is relevant if you're operating in multiple EU member states. Refer to the EU's Article 29 working party guidance for help. ☐

10. **Comply across multiple geographies:** Check the clarity of any contracts with EU member states within the EU, and individual laws for any countries falling outside the EU. ☐

"GDPR is an opportunity to provide a safer customer experience for our retail partners here in France. We understand it as a way for them to build reliable and trust-based relations with their customers. Relationships that starts well-ahead of the store experience and the point of sale. Gathering information regarding logistics and delivery time can be critical for retailers to improve the customer experience, and improvement in warehouse processes can also be used to customise the shopping experience." | **Richard Bogalho, Logistics Solutions FR, Panasonic Business**

11. **Update policies and procedures:** Making sure they reflect the correct use of CCTV according to the GDPR ☐

12. **Follow the right CCTV Codes of Practice:** Ensure all teams are working within the most recently published codes. ☐

13. **Carry out a full security audit of your CCTV security system:** Include reviewing access rights, remote security, and accessibility of systems. Update passwords and implement a strong process to ensure these and system updates are refreshed regularly. ☐

14. **Update all software and hardware:** All maintenance contracts and agreements should include the application of technology updates. ☐

15. **Store business data separately to the CCTV network:** Set a process in place for business data to be stored and accessed separately. ☐

16. **All new technology should comply with a Data Protection Impact Assessment (DPIA):** Put a DPIA in place for the completed consideration and implementation of any new technology – such as body cameras. Seek the advice of the ICO should the related data processing be deemed high risk. ☐

17. **Check through the 8 data protection principles of GDPR:** Principle #7 highlights the protection of data - CCTV systems and all relevant data should be appropriately secured against cyber-attacks and other security threats. ☐

18. **Familiarise and review:** Make sure you and your teams have read the ICO's paper "Preparing for the GDPR, 12 steps to take now" and reviewed the updated Data Protection Directive. ☐

19. **Document any concerns and steps taken to ensure compliance:** The ICO has advised it will give consideration to Retailers that actively communicate concerns with case workers, and demonstrate evidence for addressing issues with the steps taken to comply with the GDPR. ☐

Further help:

A live chat feature is available via the ICO website, where questions can be asked. A transcription of conversations is available following discussions.

The ICO encourages Retailers to sign up to its weekly newsletter and read its' blog for current developments and any announcements related to the GDPR and the Data Protection Directive

INDUSTRY EXPERT BOARD

Our board of European industry experts regularly brings together decades of experience, insights and opinions to support leaders and decision makers from the retail industry.

Gary Byrne
Head of Retail Solutions UK at Panasonic Business

My focus is to understand my customer's business drivers and operational needs, in order to support and advise on the optimum technological solutions to enhance the customer experience and increase operational efficiency.

This involves taking a consultative approach to develop value-driven technology propositions that drive long-term relationships and revenue for my customers.

Contact details:
Phone: +44 799 052 39 85
Email: gary.byrne@eu.panasonic.com

linkedin.com/in/gary-byrne-8a680640/

Ye-Un Lee-Strasburger
Business Development Europe at Panasonic

Digital innovations are redefining the shopping experience like never before, from customer engagement to operational analytics.

I work with colleagues across Europe to focus first on the business challenge presented, and then identify which proven technology will best meet the needs of both the client and regulatory laws.

Contact details:
Phone: +49 611 235 259
Email: Ye-Un.Lee@eu.panasonic.com

linkedin.com/in/yeunlee/

Richard Bogalho, Head of Logistics France at Panasonic Business Europe

The logistics industry has a great wealth of opportunity today to capitalise on innovative technologies such as artificial intelligence, next-generation automation and IoT to ensure a positive customer experience and gain long-term loyalty.

My goal is to help customers improve their transport and supply chain businesses by ensuring they become more efficient and sustainable.

Contact details:
Phone: +33 609 084 99
Email: Richard.Bogalho@eu.panasonic.com

linkedin.com/in/gary-byrne-8a680640/

Panasonic
BUSINESS

To learn more about Panasonic's GDPR friendly technology:

Visit: **Panasonic Secure Communication**:
business.panasonic.co.uk/security-solutions/secure-communication

Visit: **People Masking Technology**:
business.panasonic.co.uk/security-solutions/people-masking-technology

Call +44 (0) 2070226530
Email info@business.panasonic.co.uk