Retail Approach to Implementing Critical Elements of the GDPR

GDPR Discussion Document for the Global Retail Industry

May 17, 2018

The General Data Protection Regulation (GDPR)[1] sets out changes to almost every area of customer data processing. Retailers with storefronts, websites, mobile apps or other digital platforms through which they serve customers face new compliance standards, additional administrative burdens and liability for violations, as well more stringent enforcement and penalties.

Since the GDPR is both industry-neutral and channel-neutral, there are no sector-specific rules about the use of customers' personal data by retailers for various commercial purposes, whether online, on mobile apps, in physical store locations or omni-channel. Customers, however, expect retailers to process personal data responsibly and seamlessly when serving them. To meet these expectations, retailers must find appropriate methods for GDPR compliance that further their customer relationships and do not frustrate them.

With the GDPR taking full effect, there are still many questions about how the GDPR applies to critical areas of retail operations, such as: using customer data for improved service or promotional opportunities, managing customer information databases and loyalty programs, collecting customer consents, and honoring customer rights to erase, or port to a competitor, a customer's personal data.

Retailers have a long history of nurturing customer relationships and meeting consumer expectations. The purpose of this document is to share this experience with GDPR stakeholders, including data protection authorities (DPAs), to facilitate retail-specific approaches to compliance that will meet the requirements of the GDPR while ensuring that retailers can continue to provide customers with the personalization, omni-channel experiences and seamless retail operations that they expect.

[1] Regulation (EU) 2016/679 adopted on 14 April 2016. The GDPR becomes enforceable on 25 May 2018 after a two-year implementation period concludes.

1. Right to Erasure

- Purpose of the rule
  - This rule was proposed to address consumers' interests in removing their personal data from databases or web search inquiries if there is no compelling reason for businesses to keep that data.
  - In the retail context, the right to data erasure is subject to certain legal and operational limitations discussed below. DPAs should recognize these limitations in their enforcement of the GDPR and in guidelines on the scope of data subject to the right to erasure.

- Retailers' interpretation

Maintaining records related to purchased goods.

  - In compliance with the GDPR, retailers will offer customers choices in how to erase their personal data that is used for certain purposes (e.g., targeted marketing), but due to the transactional nature of product purchase data, retailers must continue to maintain records of goods purchased by their customers.
  - Erasing transactional data necessary to prevent fraud or reconcile card transactions, or to permit customers to return or exchange products, would frustrate customer expectations. It would also harm customers who could not later obtain a refund for unwanted products, or who could not exchange a product to maintain its value to the customer (e.g., exchange clothing so it is the right size).
  - To better serve customers and meet their expectations, retailers should not erase product purchase data that would weaken fraud protections or prevent payment reconciliation, product returns or product exchanges.
    - Purchase records are critical to serving customers who seek to make returns or exchanges, and to assisting them on purchasing or exchanging related items (i.e., in the same style or series). For example, some records must be maintained for a period of time to reconcile payment card transactions, or to complete product returns or exchanges.
    - Operationally, retailers need to retain data related to transactions for fraud detection or prevention, investigative or litigation purposes.

Compliance with legal obligations.

  - Retailers appreciate that the GDPR takes into account that the right to erasure cannot apply to data that they are required by law to maintain as

records of transactions. For example, some national laws require retailers to maintain transaction records for up to 10 years. Retailers cannot erase this data without violating these laws, and the GDPR should be interpreted and applied in a way that does not require violation of any national laws in order to comply with customer erasure requests.

- Similarly, retailers appreciate that the GDPR recognizes they cannot be responsible for ensuring data erasure when a government authority has legally requested or ordered it to provide the personal data as part of a government investigation or for other authorized purposes. Once the data is in the control of a government enforcement authority, agency or court, a retailer cannot ensure its erasure on systems outside of its control and may also be prohibited by the governmental authority from erasure of the data on its own system.

Customers' data on social media and review sites (third-party platforms).

- Customers who ask a retailer to remove personal data from the retailer's systems would not reasonably expect the retailer to follow the consumer online and erase data the consumer has voluntarily placed elsewhere.
- Third-party platforms, such as social media and consumer review websites, may post public comments from a consumer about a retailer, but the controller of that posted information is the platform operator, not the retailer.
- The GDPR's right to erasure therefore should not be construed as an affirmative obligation for retailers to follow customers' postings of personal data wherever that data appears online (e.g., on social media or consumer review websites) to facilitate consumer erasure requests. Rather, third-party platforms that post public comments of consumers are the controllers of that information and have the principal obligation to erase personal data upon the consumer's request.

Compliance with customers' erasure requests.

- Successful retailers know that consumers expect them to innovate and deliver new content including consumer trends, top sellers, and the latest product or fashion developments. One way that retailers meet this customer expectation is by using and sharing aggregate or processed data that has been rendered non-personal data and is not subject to GDPR erasure requirements, including anonymized, aggregate customer data and data generated from personal information that does not identify a data subject.
- Some retailers may use deidentification tools to extract personal data from non-personal data sets that it retains for transactional, legal or other

purposes. Consumers submitting erasure requests related to their personal information would not expect the retailer to erase information that no longer identifies them. Deidentification tools are just one of the methods available to retailers that enable compliance with erasure requests related to their personal data while preserving use of non-personal business data necessary for the retailer to maintain competitive operations.

- The right to erasure should not cover technical operations necessary to ensure the security of the relevant data, and should not apply to data captured in unstructured and unsearchable systems (e.g., closed circuit security footage). Erasing data that leaves security systems vulnerable would be antithetical to data protection requirements to ensure customer data security, and the right to erasure should not extend that far. Additionally, the right to erasure should not require retailers to pull together data in unstructured systems to eliminate it; this would risk creating greater amounts of associated customer data which would be contrary to the data minimization principles in the GDPR.
- Businesses should be allowed to keep appropriate records of data erasure requests for evidencing accountability and demonstrating that they have complied with individuals' requests for data erasure.
- Retailers and customers should understand the above legal and operational limits on what data is appropriate to be erased under the GDPR's right of erasure and preserve the data necessary to fully meet customers' expectations.

2. Right to Data Portability

- Purpose of the rule
  - This rule was proposed to protect consumers' interests in moving valuable account information (e.g., utility usage, subscriber data) or media (e.g., photos, documents) stored on one online service to a similar service provider.
  - In the retail context, retailers and consumers reasonably expect the right to data portability to be applicable to data that is *not* transactional in nature (i.e., data that must be maintained by the retailer) for the same reasons discussed above under the right to erasure. Additionally, retailers should recognize that the right to data portability covers *personal* data and does not extend to proprietary retail business information that, if required to be ported, could raise unfair competition concerns.

- DPAs should recognize these limitations on the scope of the right to data portability in its enforcement of the GDPR and in its guidelines on the proper scope of data that is subject to this right.

- Retailers' interpretation
  - Retailers should continue to maintain the confidentiality of any data related to its customers (e.g., information related to a loyalty plan) that is *neither* provided directly by the customer *nor* user-generated stored media (e.g., photos created by the customer and uploaded to the retailers' system).
  - Retailers appreciate that the right to data portability covers only *personal* data of a customer and not data that is derived from transactions or constitutes analytical inferences made by businesses from the behavior of their customers (e.g., shopping habits / behavioral analytics).

Decoupling personal data (for porting purposes) from competitive or commercially-sensitive retail transactional data.

- When a customer's personal data and retail transactional data are associated, the right of portability should only extend to the personal data that can be decoupled from the competitive or commercially-sensitive transactional data, and that personal data should be ported without the portion constituting transactional data.
  - Retail business data should not fall within the scope of a customer's right to data portability, which was adopted as part of the GDPR to ensure that consumers could move their *personal* data to another business.
  - Requiring businesses to port competitive or commercially sensitive data to another competitor would go beyond the purposes for which the right was adopted.
  - If the right were to also cover associated transactional data along with consumers' personal data, it would raise significant competition concerns for retailers as it could reveal product sales strategy, trade secrets and other commercially sensitive business data to any competitor that receives the ported data.
  - Additionally, if such business data is included in this right, it is likely that unscrupulous competitors would abuse a customer's right to data portability by encouraging them to request the porting of competitive information from another retailer in return for receiving lower-priced products as compensation for requesting that transfer of business data.

Compliance with customers' data portability requests at time received.

- To practically comply with the GDPR, retailers must view the data portability request from customers as occurring at one moment in time and requiring porting of covered personal data that the retailer has in its possession at that time.
- The right to data portability should not create an ongoing requirement to periodically port to another party the customer's personal data accumulated since the time of the previous request. Such a requirement may not only be inconsistent with the customer's intent and future desires, but also would set up an unreasonable, perpetual porting obligation that would be too costly to maintain.

3. Consent

- Purpose of the rule
  - The rules regarding consent were proposed to ensure that a customer ("data subject") has freely given his or her permission to a business ("controller") to process the customer's data for a specific purpose.
  - The guidelines for consent adopted by the Article 29 Data Protection Working Party (WP29) state: "Consent remains one of six lawful bases to process personal data, as listed in Article 6 of the GDPR. When initiating activities that involve processing of personal data, a controller must always take time to consider what would be the appropriate lawful ground for the envisaged processing."[2]
  - Retailers have found that other lawful bases are appropriate grounds under the GDPR for most of the processing of customer data they can envisage, however, consent may be necessary for some processing or as an *additional* basis on which to ensure their processing of data is valid.

- Retailers' interpretation
  - Established retailers have obtained the consent of data subjects to process their personal data for specific purposes for many years, and in some cases, several decades. As guidelines on consent are further developed by DPAs, retailers' views on how to implement consent in the retail context can be instructive to DPAs as they consider scenarios in which the GDPR requires consent.

[2] See *Guidelines on consent under Regulation 2016/679*, adopted on 28 November 2017, as last revised and adopted on 10 April 2018 (http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051).

Validity of prior consents.

- Retailers and consumers reasonably expect to rely upon prior consents obtained in compliance with existing laws before 25 May 2018 where a customer had *freely* given his or her permission to a retailer to process the customer's data for a *specific purpose*.
- Retailers support the WP29 guidelines' view that the GDPR's four consent conditions, coming into effect on 25 May 2018, are required for obtaining valid consent *on or after* that date. Because the GDPR's requirements cannot be retroactive, retailers call for clarification that the absence of providing its four customer notification requirements when a retailer validly obtained customer consent on a prior date *does not invalidate* the prior consent.
- Consumers expect, and retailers agree, that consents validly obtained under the 1995 Data Protection Directive should remain valid and *should not require* the customer to resubmit the same consent. (Similarly, as noted below, consents validly obtained under the e-Privacy Directive *should remain valid* pending adoption of new rules in the EU's forthcoming e-Privacy Regulation.)
- Requiring companies to re-obtain consent where it was validly obtained before for the same purpose is also counterproductive because it places enormous burdens on consumers, not just businesses.
    - For example, if re-obtaining consents in these situations is required for retailers, customers could face hundreds of new emails, phone calls or mailed notices asking for their reconfirmation of prior consents for the same purposes.
    - Additionally, customer re-consent in the physical retail space could add unnecessary time to each transaction – inconveniencing consumers who prefer to shop in stores instead of online.
    - These consequences run counter to: (i) sound public policy that seeks to minimize the number of solicitations consumers receive; and (ii) an enhanced, customer experience that is intended to be more pleasant, streamlined and efficient for consumers.
    - For these reasons, valid prior consents should be relied upon by retailers and their customers, and re-obtaining consent for the same data processing purposes should not be required.

Application of GDPR to valid consent under e-Privacy Directive.

- A related issue regarding the validity of customer consents previously obtained under existing law is raised by the unclear text of the final

paragraph of section 1 of the WP29's guidelines on consent with respect to the application of the GDPR consent conditions to situations falling within the scope of the e-Privacy Directive (2002/58/EC). The text in this paragraph states that the GDPR consent conditions are "preconditions for lawful processing," but are "not considered to be an 'additional obligation'" prohibited by Article 95 of the GDPR. Retailers find this language confusing in light of the continued operation of the e-Privacy Directive pending the adoption of the forthcoming e-Privacy Regulation that will replace it.

- The WP29's consent guidelines could be interpreted to require businesses to apply the GDPR consent conditions *retroactively* to previously obtained customer consents that presently fall within the scope of the e-Privacy Directive. In our view, any new conditions for consent not presently required by the e-Privacy Directive would amount to additional obligations that are prohibited by Article 95. Retailers have therefore called for clarification from DPAs that additional steps are not required to validly obtain consent under the currently effective e-Privacy Directive, and that the GDPR does not automatically invalidate the consents previously validly obtained under the e-Privacy Directive prior to adoption of the forthcoming e-Privacy Regulation.
- Retailers have a practical concern with the application of the GDPR consent conditions to situations falling within the scope of the current e-Privacy Directive and that will again fall within the scope of the forthcoming e-Privacy Regulation. Retail businesses anticipate that certain data processing practices will need to be updated to comply with the new e-Privacy Regulation once it is adopted, and they are concerned that the guidelines require business practices to be updated twice: first, to add GDPR consent conditions to obtain valid consent under the e-Privacy Directive prior to adoption of the e-Privacy Regulation; and second, upon adoption of the e-Privacy Regulation (particularly if additional legal bases or conditions for processing are adopted).
- Requirements to serially change business practices over a short period of time to obtain valid consent for processing – through adoption of new consent practices for a short interim period before adopting different, long-term compliance practices – will needlessly complicate business efforts to comply with both the GDPR and e-Privacy Regulation. Retailers believe it will also create additional confusion for their customers who may, as a result, receive multiple solicitations seeking their consent for the same process within a short time (when the e-Privacy Directive is later replaced by the e-Privacy Regulation).

- Retailers would appreciate further efforts by DPAs to clarify the interpretation of the GDPR for compliance purposes to ensure that retail businesses validly obtaining consents under the current e-Privacy Directive – using practices for obtaining such consents as currently implemented – may continue to rely upon the validity of those consents at least until the establishment of new consent requirements upon the adoption of the forthcoming e-Privacy Regulation, provided that in the interim the consented-to processing activities remain unchanged and that reasonable withdrawal of prior consents remains available.
- Finally, retailers acknowledge that the relationship between the GDPR and the e-Privacy Directive has not yet been fully harmonized. This follows from GDPR Recital 173 which states that the e-Privacy Directive must be reviewed *and amended* for purposes of ensuring the e-Privacy Directive's consistency with, and clarifying its relationship to, the GDPR. Until businesses receive the clarity and consistency called for by the GDPR, we respectfully ask DPAs to defer their inquiries into business practices that are currently in compliance with the e-Privacy Directive.

Retail considerations for consents obtained in compliance with GDPR.

- Where relying on existing consents is not possible and consents need to be refreshed, a retailer's notice or request to consumers to update their consent should not be considered a direct marketing communication.
- With respect to consents obtained for multiple store brands under the control of one retail company, a global consent process may be used so that the retailer is not required to obtain separate consents for the same process for each brand under its control, provided that the customer is informed of all store brands to which she is giving her consent.
- If crafted in a way that clearly does not limit other methods to comply, retailers would evaluate the efficacy of a single, comprehensive process to collect consent, applicable to the retail context, that is compliant with the consent requirements of the GDPR.

Relying on consent obtained by other controllers.

- With respect to consents required to be obtained by a retailer from customers using a retail store's mobile app, retailers should be able to rely upon the standardized mechanism in the mobile app platform (e.g., Apple's App Store, Google's Play Store) to demonstrate that the consent to download and install the app, and to activate certain app features (e.g., location tracking), was informed and freely given for the specific purpose of using the app.

- Retailers cannot alter the app market's process by which a customer consents to download and install a mobile app on a smart phone, and must therefore rely on the app market's or smart phone's standard consent process as evidence that the customer validly consented to download, install and activate the mobile app.

4. Other Legal Bases for Retail Processing of Customer Data: Legitimate Interest and Contractual Necessity

- Purpose of the rule
  - The GDPR's six legal bases for processing allow flexibility in how companies may use personal data for their own business purposes while ensuring individuals' rights are respected.
  - As noted in section 3 above, there are five other legal bases for processing data under the GDPR that retailers may rely upon other than a customer's consent. Retailers may therefore determine that they already have a legitimate interest or contractual necessity, among other legal bases, to process customer data for common retail purposes.

- Retailers' interpretation

Ensuring seamless shopping experience for customers.

  - Customers expect retailers to process their data when it is a necessary component of the underlying retail shopping experience. Consumers do not expect retailers to interrupt their shopping, or serially notify them, simply to obtain their affirmative consent for every aspect of the retailer-customer interaction that requires some type of data processing.
    - Such a practice would be very disruptive to the customer's shopping experience, whether online, mobile or in-store, and customers would likely reject it as annoying and unnecessarily burdensome on them.
  - To meet customers' expectations of a seamless shopping experience based on responsible data use, retailers may rely upon other legal grounds to process customer data, such as in cases where they can demonstrate a legitimate interest or contractual necessity to process customer data.
    - The examples are as varied as the number of consumers and retailers, but customers understand that retailers' collection, use and retention of personal information is part of an individualized retailer-consumer experience.
    - Therefore, under the GDPR, absent consent, retailers would ensure having a legitimate interest in, or a contractually

necessary basis for, processing customer data and that the purpose for the data collection, the duration for which it is retained and other elements that constitute lawful processing are met in a manner that is most appropriate for consumers in the retail context.

Loyalty programs and common in-store transactions.

- A common retailer-customer experience where neither the consumer nor the retailer would expect serial consent solicitations to be required is for promotions or discounts received from retail loyalty programs in which the consumer enrolls. Retailers may justify such data processing on other legal bases under the GDPR. Loyalty programs may be distinguished from marketing or profiling communications that otherwise might require consent.
- Additionally, many common in-store transactions, where requesting consent could be disruptive to the shopping experience, may be lawfully grounded on the bases of legitimate interest or contractual necessity.

Other retailer considerations for lawful processing.

- If crafted in a manner that would not limit other ways to comply, retailers would evaluate the use of a uniform approach to what constitutes "legitimate interest" or "contractual necessity" in the retail context.
- Retailers also call for a coherent implementation of the legitimate interest and contractual necessity grounds to avoid conflicting regulatory requirements for processed data if these legal bases are not adopted as lawful grounds for processing data under the EU's forthcoming e-Privacy Regulation.

5. Data Breach Notice

- Purpose of the rule
  - This rule was proposed to create incentives for businesses to improve their overall data security practices and to give regulators greater oversight over data security risks and breaches.

- Retailers' interpretation
  - Retailers support breach notification for *all* businesses suffering breaches of customer data.

Breaches suffered by co-controllers of data.

- Retailers would appreciate a recognition by DPAs that certain breached service providers are data controllers in their own right and effectively operate as co-controllers of the retail customer's payment card data. As controllers themselves, these service providers should make the required notices to regulators and individuals of their own breaches.
    - Some data processing by third parties to retailers, such as card payments services, involves massive amounts of cardholder payment processing where relatively few payments services providers and branded card networks collect and route payments for millions of retailers.[3]
    - When breaches are incurred by these and similar one-to-many service providers, individual retailers are neither in position to know the circumstances of the breach nor determine if it is likely to create a high risk to individuals' rights.
    - Furthermore, placing the notice requirement exclusively on the unbreached retailers alone in these multi-party scenarios could trigger the delivery of thousands of separate breach notices to regulators for the single breach. If notice to affected individuals is also required, customers could conceivably receive dozens of notices about the same service provider's breach, with the content of each notice likely being different (due to incomplete information provided by the breached entity to thousands of unbreached retailers making notice).
- Recognizing such service providers as data controllers in these and similar one-to-many service provider scenarios would prevent the potential massive over-notification of regulators and affected individuals for a single breach, and the resulting consumer confusion created by this type of data breach notice rule where such recognition is not made by DPAs.

Breach notice time limits.

- Retailers support reasonable and practical time limits to make required notices, where the clock starts running only when the party with the notice obligation first learns of the breach. (This interpretation would

[3] Consistent with the WP29's previous opinion on controllers (*see:* WP29 Opinion 1/2010 on the concepts of "controller" and "processor" adopted on 16 February 2010), these payment service providers (PSPs) are data controllers, in their own right, because: (i) PSPs have complete discretion in how to process card payments so long as they complete a card transaction for a retailer in a timely manner; (ii) nearly all retailers have no contractual authority to actively monitor the level of service (other than completion of a transaction) or audit the card data processing by PSPs; and (iii) data subjects' expectations when offering a card for payment is that they are initiating a financial transaction that sends the card information to their bank for authorization and they do not expect the retailer itself to complete this transaction unless it is the issuer of the card they use.

enable data controllers to make timely notice where a data processor unreasonably delays notification of its own breach to the controller.)

- Retailers support the interpretation that a notification obligation is triggered when a business has actual knowledge or confirmation of a breach, not merely a suspicion. Notifying unnecessarily in circumstances with no actionable information, and where no risk of harm to individuals has been established, could potentially overwhelm both individuals and regulators.

Breach notice template.

- To ensure uniform enforcement, retailers would support a voluntary template that indicates information to be included in a breach notice.

6. Automated Decision-Making, including Profiling

- Purpose of the rule
  - This rule was proposed to ensure that individuals are not subject to a decision affecting them uniquely that is based *solely* on automated processing and that any such decision will be reviewed if it produces adverse legal effects or other similarly significant effects.

- Retailers' interpretation
  - Retailers and consumers understand that customized advertising and offerings rely on automated tools and automated decision making.
  - Retailers support the interpretation in the WP29 guidelines on automated decision-making that, in many cases, customized advertising does not typically have a significant effect on individuals. For this reason, most online customized advertising does not require consent, which is consistent with consumers expectations as well.
  - Retailers should evaluate whether and when automated decision-making might produce unintended discriminatory consequences, especially regarding pricing, that may require informed consent.
  - Retailers appreciate confirmation by DPAs that the scope of the profiling provision is limited to actual decisions, which relate to a specific individual, rather than any data analytics used, for instance, to improve customer services without making a decision in relation to a specific individual.

Inquiries about this GDPR Discussion Document may be directed to:

Joanna Lopatowska
Adviser, Consumer Policy & Digital
EuroCommerce
lopatowska@eurocommerce.eu

Paul Martino
Vice President, Senior Policy Counsel
National Retail Federation
martinop@nrf.com

About EuroCommerce

EuroCommerce is the principal European organization representing the retail and wholesale sector. It embraces national associations in 31 countries and 5.4 million companies, both leading multinational retailers such as Carrefour, Ikea, Metro and Tesco, and many small family operations. Retail and wholesale provide a link between producers and 500 million European consumers over a billion times a day. It generates one in seven jobs, providing a varied career for 29 million Europeans, many of them young people. It also supports millions of further jobs throughout the supply chain, from small local suppliers to international businesses. EuroCommerce is the recognized European social partner for the retail and wholesale sector. www.eurocommerce.eu

About NRF

The National Retail Federation is the world's largest retail trade association. Based in Washington, D.C., NRF represents discount and department stores, home goods and specialty stores, Main Street merchants, grocers, wholesalers, chain restaurants and internet retailers from the United States and more than 45 countries. Retail is the largest private-sector employer in the United States, supporting one in four U.S. jobs — 42 million working Americans. Contributing $2.6 trillion to annual GDP, retail is a daily barometer for the U.S. economy. www.nrf.com