WHITE PAPER

HOW RETAILERS CAN DEAL WITH THE NEW REALITY OF GDPR

A careful strategy and effective solutions can help businesses overcome this compliance hurdle.

EXECUTIVE SUMMARY

The European Union changed the global face of privacy regulation with the implementation of the General Data Protection Regulation (GDPR) in May 2018. This sweeping regulation governs the privacy of personal information belonging to EU residents and applies to that information worldwide, not just within the boundaries of the EU.

Retailers around the world must re-engineer their business processes to comply with this regulation or face significant penalties, ranging up to 4 percent of worldwide revenue for a single violation. These massive fines can affect the bottom lines of even the largest companies, attracting the attention of CEOs and board members.

Retailers who haven't started their GDPR planning should immediately work to determine how the regulation affects their operations. The best way to do this is to assess current practices and controls against GDPR requirements and then work to close any gaps identified by the assessment. Fortunately, several key solutions and services can assist with this remediation, including encryption technology and strategic consulting services.

What Is GDPR, and How Does It Affect Retailers?

GDPR is a comprehensive privacy regulation designed to give residents of the European Union control over the use and sharing of their personal information. Passed by the European Parliament in April 2016, GDPR came on the heels of public outrage over government surveillance. The law included a two-year grace period, allowing organizations time to revise their business practices and implement appropriate controls.

What Does GDPR Require?

GDPR requires that organizations incorporate data protection and privacy controls in all of their activities. Article 25 of GDPR summarizes the philosophy behind GDPR when it calls for "data protection by design and by default." While organizations may take cost and other contextual information into account, the bottom line is that they must implement technical and administrative controls that are designed to protect the privacy of personal information.

Organizations subject to GDPR may not process personal information unless they have an explicit lawful basis for doing so under one of the following six provisions:

1. The data subject has provided explicit consent to the processing for a specific purpose.
2. The processing is necessary to comply with a contract agreed to by the data subject or as part of entering into a contract at the request of the data subject.
3. The processing is necessary to comply with a legal obligation of the processor.
4. The processing is necessary to protect the vital interests of the data subject or another person.
5. The processing is necessary for carrying out tasks in the public interest or in the exercise of official authority vested in the processor.
6. The processing is necessary for the purposes of the legitimate interests pursued by the controller or a third party, except where those interests conflict with the interests, rights or freedoms of the data subject.

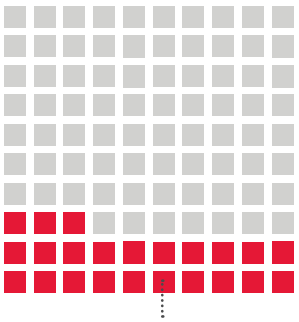
Many organizations choose to undertake data processing by exercising the first of these provisions: informed consent. It is important to note that this must be explicit consent, where the data subject affirmatively opted in to a specific use of data. Organizations cannot comply with GDPR while using opt-out approaches or asking subjects to agree to sweeping statements about data processing. GDPR also requires that organizations provide a process for individuals to revoke consent that they've already granted, access their own personal information and demand that organizations erase stored information, with some exceptions. This last provision is commonly known as the "right to be forgotten."

Who Is Affected by GDPR?

While GDPR is European law, its provisions have global reach. GDPR specifically claims jurisdiction over companies handling the personal information of EU residents wherever it may exist in the world. Under this provision, a company operating entirely within the U.S. is included in the scope of GDPR compliance if it conducts business in the EU or otherwise handles the personal information of EU residents.

Some companies may be able to make a reasonable argument that EU authorities have no jurisdiction over them and, therefore, will be unable to mandate compliance or assess fines. However, the global nature of most businesses means that almost every organization will have some nexus of business in the EU that provides jurisdiction. There are many unanswered questions regarding GDPR jurisdictional issues that will only become clear as the courts establish case law.

Retailers, in particular, should be concerned about the scope of their GDPR compliance. Retail is arguably the industry most affected by these EU requirements due to the volume of personal information handled. This is compounded by the fact that retailer records often include credit card information, which is among the most sensitive types of information covered by the privacy regulations.



23%

The percentage of organizations that have no formal privacy function[1]

Penalties for Noncompliance

The potential fines for organizations that fail to comply with GDPR can be quite steep and are the cause of significant concern for organizations of all sizes. The fines are progressive in nature, designed to have a substantial impact on any organization, regardless of its size.

Regulators have wide discretion when assigning penalties under GDPR, and have several important tools at their disposal. For minor, first-time offenses, they may opt to simply warn a business that its practices are out of compliance and that the business must remediate the situation to avoid facing penalties. They may also prescribe compliance audits on a one-time or recurring basis. The major sanctions of GDPR are its financial penalties, which are capped at €20 million (roughly $23 million U.S.) or up to 4 percent of a company's total revenue, depending on the nature of the offense.

Regulatory agencies in each EU nation are outlining their enforcement priorities under the new regulation. For example, the French data protection authority acknowledged the difficulty of total compliance and said that it will take that into account in its enforcement actions. Dutch authorities have stated that fines will be imposed only when something is very wrong. The general opinion among compliance professionals is that retailers and other businesses that demonstrate good faith efforts at working toward compliance will likely avoid the most severe sanctions under GDPR, at least for the next year or two.

GDPR for Retailers

In addition to the obvious implications for information they store and collect themselves, retailers also face potential changes in their relationships with partners. For example, many retailers

Source: [1]Deloitte, "The time is now: The Deloitte General Data Protection Regulation Benchmarking Survey," November 2017

proactively collect a customer's location, activity, payment type, time of purchase and other protected information. Under comarketing arrangements, they may currently share this information with vendors or even sell it to marketing firms. Those arrangements now fit squarely inside the scope of GDPR and may not continue without obtaining explicit customer consent.

Retailers should also remember that GDPR applies to information collected both offline and online, and that they might collect information in unexpected places. For example, a retailer's transaction database will clearly contain personal information from electronic commerce and in-store purchases. Web servers, however, also may store logs that contain GDPR-protected data elements, such as IP addresses, page view histories and geolocation data. Retailers must carefully and thoroughly assess all of their data collection practices, including those that might be inadvertent.

The Challenges of GDPR

GDPR presents some unique challenges to retailers seeking to build compliant privacy practices. These include the implementation of data handling practices, the development of new security practices, handling customer requests for information and increased costs. Each of these areas may heavily influence how retailers approach initial and ongoing GDPR compliance.

Data Handling Practices

Retailers must scour all their existing business processes to identify areas where they store, process and transmit protected personal information. Common areas requiring compliance assessment in retail organizations include transactional databases, customer loyalty programs, credit card processing systems, email marketing efforts and business analytics programs. Prior to GDPR, the privacy burden facing most retailers was limited to credit card information protected under PCI DSS. Compliance efforts now extend well beyond this base to any personally identifiable information used for transactions, marketing or other purposes.

As organizations move toward GDPR compliance, they must adopt a philosophy of transparency that embraces communicating with consumers about the collection, storage and use of their information. This may be the biggest philosophical shift for retailers who traditionally collected blanket consent on an opt-out basis rather than explicitly requesting permission for each data processing activity.

Security

GDPR encourages organizations to reduce security risk and their compliance burdens by eliminating personal information as much as possible. Tactics for achieving this goal include minimization, pseudonymization and anonymization.

Minimization practices direct organizations to collect and maintain only information that is necessary to perform a legitimate business function, and to destroy that data as soon as it is no longer required for an approved purpose. Minimization not only ensures that an organization complies with its notice and consent requirements, but also reduces the impact of a successful data breach. The smaller the amount of data that an organization stores, the fewer individuals that will be affected by a breach.

Pseudonymization replaces personally identifiable information in a data store with artificial identifiers, or pseudonyms. For example, a retailer might maintain customer records for marketing analytics but remove identifiable information such as the customer's name, street address, telephone number and email address, replacing those fields with a unique customer identifier. Pseudonymized records may make use of encryption technology to render personal information unreadable except by

GDPR Breach Notification

Organizations suffering a breach of information covered by GDPR must comply with the EU's rigorous breach notification requirements. The law requires that any data controller suffering a breach report the circumstances to its national authorities "without undue delay" — specifically stating that notice should take place within 72 hours of breach detection, if feasible. A controller who does not provide notice within that initial three-day period must explain the reasons for the delay.

Breach notices must include four elements of information:

- Nature of the breach, including the type and quantity of information and people affected
- Name and contact information for the firm's data protection officer
- Likely consequences of the breach
- Measures taken or proposed to address the breach and mitigate its adverse effects

Most retailers who operate within the U.S. are already subject to state data breach notification laws, as well as credit card notification rules under the Payment Card Industry Data Security Standard. In most cases, retailers will be able to adapt those existing notification procedures to cover GDPR requirements. This is the preferred approach, as it allows organizations to seamlessly integrate breach notification requirements with their existing cybersecurity incident response process.

authorized users. One key attribute of pseudonymized records is that the pseudonymization may be reversed if necessary.

Anonymization takes this practice further by removing personal information from records in an irreversible manner. Privacy analysts go through the same process of locating any personally identifiable information, as they would when performing pseudonymization, but they then remove that information completely from the record without replacing it with a random identifier. It is not possible to reverse a properly designed anonymization process.

Customer Requests for Information and Erasure

Under Article 15 of GDPR, consumers have the right to request that retailers provide them with copies of all of the personal information maintained about them by the business. This may introduce a significant burden for retailers who store data in disparate systems. GDPR compliance efforts must include identifying all places where personal information is stored and implementing a mechanism for retrieving information from those sources and providing it to consumers upon request. Most privacy officials interpret this rule as excluding anonymized information, adding to the importance of anonymizing as much information as possible.

In addition to the right to receive copies of personal information, Article 17 of GDPR provides consumers with the so-called "right to be forgotten." This allows consumers to request that data controllers purge their personal information from data processing and storage systems. With some exceptions, retailers must then purge that information "without undue delay."

Assessing GDPR Compliance Status

Retailers have several options at their disposal for assessing their existing GDPR compliance status, identifying any gaps and implementing remediation measures. Some organizations may choose to conduct this assessment internally, using their own security, privacy and compliance professionals. Others may opt to bring in a consulting firm to assist with the work. These engagements may include vendors with specific experience focusing on retail GDPR compliance projects.

Increased Costs

It's likely that any retailer subject to GDPR will complete its gap assessment with the conclusion that it must implement new controls to fully comply with the law. Completing the assessment and implementing any required controls will undoubtedly raise an additional challenge: increased operating costs.

In addition to the costs associated with becoming compliant, retailers will find that they also have ongoing expenses associated with GDPR compliance. This includes the salary of the digital protection officer and, if applicable, that person's support staff. It also includes the costs associated with monitoring the organization's compliance status, fulfilling consumer data export and erasure requests and maintaining and supporting technical compliance controls.

As organizations develop estimates of these new costs, they should work them into regular, recurring budget items to ensure that compliance efforts don't cause financial surprises down the road.

The Road to GDPR Compliance

Retailers should recognize that getting to GDPR compliance is not a rapid process. Depending on the complexity of the organization and the state of current security and privacy controls, it may take a year or longer to achieve initial compliance. Once a retailer does achieve initial compliance, maintaining compliant status requires an ongoing investment of time and money in maintaining, updating and monitoring the security and privacy of customer information.

Retailers should plan to work with their own technology

Compliance Solutions

Retailers have a wide variety of technical solutions available to assist with GDPR compliance efforts. These technologies help track compliance projects, securely store data and protect transmitted information from prying eyes.

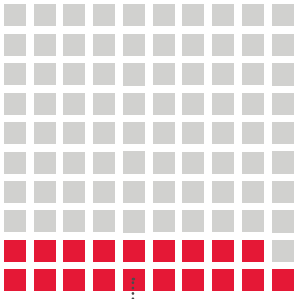
Governance, risk and compliance (GRC) solutions provide a centralized monitoring system for all an organization's compliance obligations. GRC tools assist with project management, map compliance requirements to specific security and privacy controls and assist with the assessment/audit and remediation process.

Storage solutions provide built-in encryption technology designed to help organizations reduce the burden of complying with GDPR's data protection requirements. These solutions assist with the management of encryption keys and ensure that private information is protected with strong encryption.

Network security tools provide protection for data in transit between an organization's sites as well as information being transferred to customers, vendors and business partners. Other tools that help an organization achieve GDPR compliance include:

- **Email encryption** to provide secure messaging capabilities
- **File transfer systems** to facilitate data exchange
- **Web security gateways** to apply strong encryption to e-commerce

and business teams as well as business partners to engage in a four-phase remediation effort that begins with building a data inventory, continues by conducting a gap analysis of existing controls, prioritizes remediation efforts and finally implements a compliant solution. This process may include multiple cycles of planning and implementation that help the organization make steady progress toward a fully compliant status. This progress provides an important demonstration to regulators that the business is committed to customer privacy and complying with GDPR.



19%

The percentage of U.S. IT professionals who feel informed about GDPR's impact on businesses[2]

Phase 1: Data Inventory

The data inventory builds the foundation for the entire compliance effort. Retailers must scour all their existing systems and business processes to identify the types of information they currently collect, store and process. This inventory should clearly identify all of the locations where the organization stores personal information, as well as the security controls that exist around that data.

At the conclusion of this process, the Data Protection Officer (DPO) should have a strong understanding of the retailer's data environment. While storage and processing may not yet be compliant with GDPR requirements, this is the first important step toward achieving that goal.

Phase 2: Gap Analysis

With the data inventory in hand, the DPO may now begin the process of conducting a GDPR gap analysis. This includes analyzing the organization's business processes to verify that all personal information is collected for a legitimate business purpose and that the organization is meeting the transparency and consent requirements of GDPR. The gap assessment should also verify that the technical controls in place provide adequate security for sensitive information.

The final product of the gap analysis should be a listing of all of the control deficiencies in the organization that might require remediation. This may include a listing of stored data elements that are not necessary for a legitimate purpose and should be deleted, gaps in the consent process requiring that the organization contact customers, policy revisions necessary to meet GDPR regulations and technical control shortcomings.

Phase 3: Prioritization and Planning

The gap assessment represents the basis for a project plan designed to move the organization to a fully compliant position. The team developing this project plan should prioritize efforts based on the cost and difficulty of each initiative, balanced against the degree of risk reduction each would achieve.

The project manager may then use this prioritized list of efforts to develop a detailed project plan that includes a listing of key deliverables and target milestone dates. The speed of remediation will depend on the priority placed on compliance by the organization and the financial and human resources available for the effort.

Phase 4: Implementation

After completing the prioritization and planning phase, the

Data Protection Officer

GDPR requires that many organizations appoint a data protection officer to oversee privacy practices for the organization. While any organization may appoint a DPO, this designation is required in cases where the organization is a governmental agency, involves regular and systematic monitoring of data subjects on a large scale, or where the organization's core activities include handling sensitive information such as health records, biometric data, political opinions, religious beliefs and criminal history.

The regulation sets out specific responsibilities for the DPO within an organization. These include:

- Advising individuals within the organization of their privacy obligations
- Monitoring compliance with GDPR
- Conducting awareness training for the organization's employees
- Facilitating GDPR audits
- Monitoring the performance of a data protection impact assessment
- Serving as a contact point for regulatory authorities

Many organizations choose to combine DPO responsibilities under GDPR with other privacy practices, including those that the organization voluntarily adopts. For this reason, it is common for a chief privacy officer to also hold the regulatory designation as the organization's GDPR DPO. This individual possesses the knowledge required to comply with GDPR and is liable for the organization's privacy practices, similar to the liability of a CFO or CEO under the Sarbanes-Oxley or Dodd-Frank financial laws in the U.S.

Source: [2]community.spiceworks.com,, "Most Will Miss GDPR Deadline: UK Most Prepared, US and Rest of EU Lag Behind," May 2018

organization moves into implementation mode. This effort will most likely include a wide variety of projects designed to revise business processes and roll out new technologies.

Many of the projects in a remediation effort will be one-time initiatives designed to achieve initial compliance. For example, the organization may need to reach out to all existing customers to notify them of privacy practices and obtain explicit opt-in consent for data processing to continue. Similarly, the organization may conduct a search of employee workstations to identify any personally identifiable information that is locally stored and transfer that data to an approved, secure location.

Other projects will build the systems and processes required to maintain long-term compliance with GDPR obligations. For example, a project might develop the process that receives and fulfills customer requests for data export or erasure. Similarly, a project might create an ongoing process for monitoring the organization's data loss prevention system.

Policy Revisions

One of the most visible effects of GDPR is the wave of emails that consumers received as the compliance deadline approached. These messages notified them of changes to website privacy policies and terms of service designed to comply with GDPR provisions and asked them to provide explicit consent for data processing.

In most cases, organizations will be able to create the required GDPR documentation by revising and supplementing their existing privacy policies. These revisions should include clear descriptions of the organization's privacy practices, as well as required disclosures of how consumers may exercise their right to access data and their right to be forgotten.

CDW: A Retail Partner That Gets IT

CDW and its solution providers can serve as your organization's GDPR compliance partners. Our large and experienced retail practice includes experts on a variety of technology challenges facing retailers and is well versed in security strategies.

CDW's long-standing partnerships with key vendors in cloud, managed hosting and hosted voice services for contact centers and customer relationship management integration allow CDW experts to take a comprehensive approach to identify and meet the needs of every customer. Each engagement includes five phases designed to help you achieve your GDPR compliance objectives in an efficient, effective manner. These phases include:

- An initial discovery session to understand your goals, requirements and budget
- An assessment review of your existing environment and definition of project requirements
- Detailed vendor evaluations, recommendations, future environment design and proof of concept
- Procurement, configuration and deployment of the solution
- 24/7 phone support and ongoing product lifecycle support

The CDW Approach

ASSESS

Evaluate business objectives, technology environments, and processes; identify opportunities for performance improvements and cost savings.

DESIGN

Recommend relevant technologies and services, document technical architecture, deployment plans, "measures of success," budgets and timelines.

MANAGE

Proactively monitor systems to ensure technology is running as intended and provide support when and how you need it.

DEPLOY

Assist with product fulfillment, configuration, broad-scale implementation, integration and training.

Explore Our Featured Partners:

Carbon Black. cisco tenable™

To learn more about how CDW can help your retail operation overcome challenges such as GDPR, visit CDW.com/Retail or schedule a consultation with a CDW expert at 800.800.4239.

CDW PEOPLE WHO GET IT™