White Paper

Five Essential Steps for GDPR Compliance

Sponsored by: Commvault

Carla Arend
March 2017

IDC OPINION

The European Union (EU) General Data Protection Regulation (GDPR) is the most significant privacy regulation update since 1995, when the original EU Data Protection Directive was launched. The update was desperately needed, as the directive predated widespread internet usage, social media, and the omnipresent smart devices and had no provisions for protection of digital data. After four years of tough negotiations, GDPR was passed in April 2016 and will take effect on May 25, 2018.

While GDPR seems to be a European matter at first glance, it actually has a global reach. Every organization that collects and/or processes data of data subjects in the EU is subject to GDPR and needs to comply. The requirements for data breach notification within 72 hours, the option for class action lawsuits, and suspension of personal data processing in case of noncompliance, in addition to fines of up to 2% of annual revenue, or €10 million, for technical infringements and 4% of annual revenue, or €20 million, whichever is bigger, for noncompliance with the fundamental principles and rights, make GDPR a boardroom issue.

With the GDPR compliance deadline in May 2018 fast approaching, organizations are now in the process of understanding which key actions they need to take, in terms of both technology selection and process readiness.

While readiness levels vary greatly, it is important to get started now, to be sure to be compliant by the May 2018 deadline, which to some organizations might seem like a Herculean task. With data dispersed across production, business intelligence (BI) and analytics, test and dev applications, and secondary storage systems for backup and disaster recovery (DR) purposes (both on-premise and in cloud applications), it can be hard to determine where to start.

Good data management practices are key to GDPR compliance success. Understanding where you have personal data (in which applications, on-premise or in the cloud, which processes use this data, and who owns it) is an important first step. The fragmentation of data stores is making it very difficult to get an overview of data and manage data efficiently. Using a consolidated data management platform helps you understand your data landscape, define and drive policy across your data estate (both on-premise and in the cloud), and of course meet the new requirements for data access, data erasure (right to be forgotten [RTBF]), and data portability.

IN THIS PAPER

This document discusses the key principles that are being put forward by GDPR and how using a data management platform enables you to address them. It provides a five-step plan to get you started on the journey to GDPR compliance by May 2018.

SITUATION OVERVIEW

GDPR has been conceived to strengthen European citizens' rights in the digital era and to make it easier for businesses to comply, as it ends the fragmentation of European data protection laws caused by its predecessor and provides one single law for the European Union member states (and associated countries like Norway and potentially also the United Kingdom after Brexit). Other countries, like Canada and South Africa, might adopt a similar regulation. It is important to understand that GDPR affects every organization globally that handles data of European citizens (which are called "data subjects" in the regulation).

GDPR sets the bar for privacy protection high, so it is important to understand some of the key principles of the regulation.

Key Principles of GDPR That You Need to Know

Rather than being very descriptive in terms of process and technology requirements, GDPR defines "principles" to ensure future relevance of the regulation. Key principles that are having the biggest implications for data management are:

- **Right to be forgotten (Article 17).** When the data subject specifically requests access to his/her data or asks for the data to be deleted, or data is no longer necessary for the purpose it was collected for, or the data subject withdraws his/her consent, the organization (data processor) needs to delete the data. While identifying the relevant data in primary applications might seem straightforward, keeping track of all copies of data in test and dev environments, business intelligence and analytics applications and, particularly, data protection and storage systems is a major task and requires good data management practices.
- **Data protection by design and by default (Article 25).** Organizations handling data of European citizens need to ensure when they review and design their processes that only the minimum amount of data necessary for the specified use case is collected and that the data is only kept for the minimum duration necessary. Processes need to be designed so that organizations always provide data protection by default. Strong data governance processes, retention management, and stringent process documentation are critical for compliance.
- **State of the art (SOTA, Articles 25 and 32).** This principle is "future proofing" GDPR, as IT technologies are developing faster than the regulator can respond. Therefore, the burden is on the individual organization to prove that it has a view on what SOTA is, in order to justify why it did or did not implement certain technologies, based on an assessment of SOTA on the context of cost, risk, and context. This understanding needs to be reviewed on a regular basis, to keep up with technology innovation. SOTA encourages organizations to implement appropriate IT solutions and develop good processes within reasonable cost, risk, and context, so that they always protect personal data in the best possible way. Investing in market-leading IT security, data protection, and analytics solutions with an innovative road map will make it easier to comply with SOTA and will also make the job of the data protection officer much easier.

- **72-hour data breach notification (Articles 33 and 34).** Organizations need to notify their data protection authority within 72 hours of them noticing a material personal data breach and provide the nature of the breach, an estimate of how many people are likely being impacted by the breach, and measures taken to mitigate the breach. For example, a lost laptop is a potential data breach. With a laptop backup solution in place, you can search the laptop and understand which data it contains, which makes it easier to understand the impact of the breach and provides important information for the data breach notification.
- **Data minimization principle (Article 25).** Keeping as little data as necessary to perform their customer services is a challenge for most organizations, given that they have a tendency to collect and keep data, just in case. Identifying and deleting redundant, outdated, and trivial (ROT) data is a key first step to minimize the data footprint and make data governance more operational and manageable. The data minimization principle needs to be balanced with other regulations, which require retention of data (health records, criminal records, etc.).
- **Defining use cases and managing consent (Article 6).** Whenever organizations want to collect data from European citizens, they have to define a clear use case for the data and get the person's consent. Once the use case ends, the data needs to be deleted. This requires an end-to-end process, from the collection of the data to the storage infrastructure, to ensure the correct data retention spans and deletion policies.
- **Data transfers (Articles 44–50).** It is important for organizations using cloud services to understand the articles on data transfers to countries outside of the European Union. Data may only be transferred to countries with similar standards in data privacy protection, like Canada. When data is transferred to countries such as the United States, binding corporate rules are recommended, although there are several other mechanisms. In preparation for this requirement, it is important to understand whether organizations have data in the cloud already, where the data resides, and which compliance mechanisms are in place.
- **Data portability (Article 20).** European citizens have the right to receive all their data in a machine-readable format, so that they can transfer it to another company. This is particularly challenging for data kept in legacy systems with proprietary file formats.
- **Accountability (Article 5).** At the core of GDPR is the concept of accountability, where both controllers and processors need to be able to document how they comply with the data protection principle and which technical and organizational measures they have put in place. Keeping records of decision-making processes about the implementation of GDPR, collecting technical documentation about products and services used, and using products with strong reporting capabilities enable organizations to demonstrate compliance with the accountability principle.

Common Challenges for GDPR Compliance and How to Resolve Them

The list of key requirements makes it clear that GDPR compliance is a challenge and will require significant process and technology updates and investments. The more fragmented the data landscape is, the more difficult GDPR compliance will be. Here are the main challenges that organizations are planning to address with technology and process investments:

- **Identification of applications that process privacy-relevant data is a key first step.** In addition, an overall *data classification exercise* is needed to understand for both structured and unstructured data, where the data resides (on-premise or in the cloud, in which countries), who owns the data, what the retention periods are, the sensitivity of the data, and whether conflicting regulations apply. This is particularly challenging for unstructured data, which makes up roughly 80% of all data. A consolidated data protection platform solution can help with this issue, as all data is indexed upon ingestion into the data protection platform and hence searchable. Data assessment and analytics can be conducted on the data protection copy of the data, without impacting the availability and response times of the production copy of the data.

- **Internal communication and education of employees about the impact of GDPR and guidelines are of paramount importance, as GDPR compliance is just as much about process improvements as it is about technology.** However, understanding data ownership helps target the critical groups of employees where GDPR awareness is most important.
- **Documentation of GDPR-related processes and decisions.** To pass a GDPR audit, you need to be able to show documentation for all your GDPR-related processes and decisions. Driving policy from a single data management platform with extensive reporting capabilities facilitates documentation.
- **Respond to data access requests and the right to be forgotten.** Driving a single policy across all unstructured data irrespective of data location by consolidating down to a single vendor for backup and archive with a single index helps drive compliance and pass audits, even in a diverse IT environment with flash storage, hyperconverged, and OpenStack-based IT systems. It also makes responding to data access and RTBF requests much easier, as all copies of a data point are accounted for. Consequently, organizations will be able to find data, correct the data, hand over the data, or delete the data upon request by the data subject within the given time frame and without the need to employ extra staff. In addition, getting your data under control brings benefits for digital transformation, business intelligence, and analytics efforts.

Best Practices for GDPR Compliance in Five Steps

The most important advice for GDPR compliance is to get started! Don't be part of the 20% of organizations waiting for further guidelines to be published or for someone in the organization to suddenly take ownership and move this forward. GDPR compliance is complex, and getting all processes into shape takes time. Five steps for GDPR compliance are:

- **Set up a cross-functional data governance team, including a data protection officer and members from IT and business leadership, that owns the responsibility for GDPR compliance and reports to the board of directors.** This team should also own the documentation of processes and decisions and policy development and do regular reviews of policies, processes, and technology choices.
- **Launch a data mapping and analytics project.** Identifying privacy-protected data across applications, servers, storage, endpoint devices, and cloud locations is the foundation for GDPR compliance. You need to know your data to govern and manage it properly. Your data store is a good place to start, as all data ultimately ends up here, and you can run analytics on the secondary copy of data without impacting performance of the primary copy of your data. Conducting a data flow analysis will shed additional light on how data moves through the organization, where copies are created, and where data ultimately gets stored.
- **Use a single platform for data governance and policy management, and extend data governance and control to cloud-based data.** Fragmented data stores, not only in primary production applications but also in secondary storage like fragmented backup and archive applications, are a key challenge to achieving and maintaining GDPR compliance. Only when you have accounted for your data and can see it through a single pane of glass will you be able to respond to data access requests and data erasure requests, understand the extent of data breaches, fulfill data portability requests and, ultimately, ensure compliance. Using a single consolidated platform for backup, archive, and data management is also key to ensure protection and availability of data.

- **Define state of the art in terms of technology attributes and processes with regard to structured and unstructured data.** Using technology from an innovative vendor will make it easier to stay on the technology evolution curve and mitigates the risk of falling behind what technology has to offer to enable GDPR compliance.
- **Develop an incident response process for communication with both the local data protection authority and with the public so that you can control what information gets disseminated once you get breached.** Having a strong data governance process and full insight into your data will help be precise in the communication.

FUTURE OUTLOOK

Preparations for GDPR compliance have only just started. While European organizations are well under way in educating themselves about GDPR requirements and starting their first initiatives, organizations outside the EU seem less aware that GDPR also applies to them, if they collect or process privacy-relevant data of European citizens.

IDC believes that the reach of GDPR will extend beyond the EU because other countries consider GDPR as the "golden standard" for data protection and also consider adoption of GDPR-equivalent laws. Countries with equivalent data privacy standards include Canada and Argentina.

CONCLUSION

If you have not started to prepare for GDPR, get started now! May 2018 is fast approaching, and getting GDPR compliance right takes time.

A good starting point is to create a prioritized list of what needs to be done. In particular, make sure that 80% of the organization's unstructured data is addressed. Devise data governance and management processes that cover data from edge devices to datacenter to the cloud.

Ensure that the organization can document its decisions and processes and can provide reports to auditors easily. In addition, choose a technology platform that helps the organization respond to data access and erasure requests as they can become a significant burden.

While this document has focused on the potential challenges that GDPR poses, IDC believes that GDPR compliance also provides a chance for organizations to differentiate through better GDPR compliance processes and can help create competitive advantage through better insight into relevant data.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com