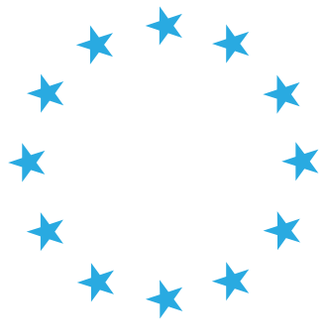
MODEL 9

Is your business affected by GDPR?



WHAT DOES GDPR MEAN FOR MAINFRAME STORAGE, ARCHIVE AND BACKUP?

On April 27, 2016, the European Union passed regulation 2016/679, more popularly known as the General Data Protection Regulation (GDPR). On May 25, 2018, GDPR implementation began, and enforcement activities started. So which organizations are affected by GDPR regulation, and what are the most difficult IT hurdles to overcome?

Though much of the public discussion about the GDPR involves the IT challenges related to compliance, the GDPR is not a regulation aimed specifically at how organizations implement IT. The GDPR is predominantly a privacy regulation that aims to give European Union citizens control over their personal data, regardless of which organizations are handling that data, or how.

When organizations seek advice on how to comply with the GDPR from experts, consultants, and vendors, they will frequently be advised to modify or enhance their IT security and data handling approaches. This is not because the GDPR specifically says that one approach or technology is superior, but rather because compliance is most simply and efficiently achieved by implementing a certain set of IT technologies and business practices.

The GDPR applies to every individual and organization that processes data about EU citizens, even if those individuals or organizations are not themselves located in the EU. As an example, an American organization that collects data on EU citizens as part of their e-commerce site is expected to comply with the GDPR. If it does not, it faces the same consequences as an organization located in the EU.

The two basic concepts underlying the GDPR are privacy by design and security by design. This means that data about EU citizens not only must be kept secure, but it also should be kept as private as possible.

A GDPR EXAMPLE

As an example of this concept, let us consider a prospective client's medical insurance declaration form kept by in an insurance company's records. As might be expected, the company is required to protect that data from hackers or insider threats that might exfiltrate data. What is new to most organizations, however, are the privacy requirements.

At a bare minimum, the GDPR's privacy rules state that access to the prospective client's records should be restricted only to the classes of user that require access to that data. So classes of users such as the underwriting and sales departments might require access to the full set of data, while administrative staff should only be able to access enough data to eventually bill the client once policy is issued, and other staff should not be able to access any information about the client at all.

Ideally, even the underwriting and sales classes of user should only have access to the client's data when absolutely required. This might mean blocking casual access to the records by these classes for any purposes other than responding to a change in condition or policy renewal.

Furthermore let's say the prospective client decided not to go through with signing up for medical insurance, she may be entitled to ask to be "forgotten"—essentially requiring the insurance company to delete the specific records containing that client's form information.

This level of privacy is not restricted to medical records. It applies to all data that can be used to identify an EU citizen. Effectively, this means all data that an organization might collect about an EU citizen, wherever in the world the organization operates or the information is kept.

REAL WORLD RISKS

Organizations are responsible for ensuring this level of privacy and security not only for the data they hold on their own on-premises IT. They are also responsible for ensuring the above level of privacy for any data they collect, store, or cause to be collected or stored on public cloud services, at service providers, and any contractors that the organization engages, anywhere in the world.

In essence, organizations cannot evade the GDPR simply by using a cloud service located in a non-EU country, or by contracting the collection and exploitation of data out to organizations not located within the EU. Great care has been taken during the drafting of the GDPR to eliminate loopholes, and the consequences of failing to comply can be severe.

Unlike many previous data security and privacy regulatory regimes, the GDPR has teeth. Fines can range up to 20 million Euros or 4% of global turnover, whichever is more. Also unlike many other governments that have enacted security or privacy regulation, the EU has a history of both being willing to legally challenge organizations, and of winning those challenges.

Several large multinationals—for example Microsoft, Intel, Apple, Qualcomm, and Google—have all been on the receiving end of EU legal actions, and the EU has given every indication that they intend to enforce the GDPR with equal or greater vigor than existing regulations.

GDPR RIGHTS

Obtaining the consent of Data Subjects to collect and process their data also plays a large role in the GDPR. That consent is expected to be granular, and consenting to broad data grabs in order to access basic services is not acceptable under the GDPR. In addition, organizations cannot collect more information than absolutely required, and it should not be held for longer than absolutely required. Furthermore, organizations must implement appropriate measures to ensure a level of security appropriate to modern risks, including encryption of personal data and ongoing confidentiality.

The above dictates means, for example, that it is no longer acceptable for an e-commerce organization to collect more information about their customers than is required for that customer to buy something on the site and have it shipped to them. It is illegal for that organization to sell that customer's information to a marketing company without that customer's consent, and it is unacceptable to present customers of the e-commerce site with a multi-page, legally dense "terms of service" that authorizes a broad data grab and resale of data in order to use the site.

The right to be forgotten is also enshrined in the GDPR, the results of which will likely affect all organizations, even those which have previously been strict about both data security and privacy. Under the GDPR, EU citizens have the right not only to view what data an organization holds on them, but to have it deleted. This includes the right to have it purged from all backups.

EU citizens also have the right to update or correct the data held on them. The purpose of this right is to ensure that, for example, improper information is not held on EU citizens by their governments, health care institutions, schools, airlines, etc., though the rules apply even to private organizations that process data on EU citizens.

EU citizens have the right to expect that once they correct data on themselves they won't have to go back and correct that data. This could be interpreted to require that data be updated throughout an organization's backups, so as to prevent a restore from overwriting the corrections someone has made. Organizations must also ensure the ongoing integrity, availability, and resilience of processing systems and services; the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and they must implement a process for regularly testing, assessing and evaluating the effectiveness of such technical and organizational measures.

The more critical the data, the more important it is for the Data Subject to be assured that their updates will hold. Complicating matters is that the more critical the data, the more likely it is that data is held on a mainframe, and there are already cost considerations as it regards mainframe backups.

PROVING GDPR COMPLIANCE IS AN UNKNOWN

Given that the GDPR is itself somewhat vague, exactly how organizations will set about proving compliance when asked remains something of an unknown. That said, since the GDPR gives EU citizens the right to see all data an organization holds on them, as well as other rights—specifically the right to be forgotten—their rights extend to backups. Similarly, organizations are to be held accountable for data breaches and inappropriate access not only of their production systems, but also of their backups. GDPR requires you to restore the availability and access to personal data in a timely manner in the event of a physical or a technical incident. That means you may be required to provide more services in DR scenarios than were acceptable in the past. For example, many organizations focus on replication as an availability solution to resume their business quickly in case of an incident. But what about access to your archives on virtual tape? Are these always available to you in every DR scenario?

When asked, it is reasonable to assume that organizations will be required to provide Data Subjects with a complete view of all the data that the organization holds on that Data Subject, including the copies/versions of information that is contained in their backups. On its own, this represents an entirely new—and significant—burden, even with the requests limited to a single Data Subject.

A formal audit of data handling practices could theoretically require the above for a random sampling of Data Subjects, as well as a complete record of every access made to the data held on those Data Subjects. Some experts have argued that these audits could include requests to identify who authorized the data access—either for specific instances, or at least who granted the rights that allowed access—and why that access was authorized. All of the above would require additional access logging, business process changes, tracking of access rationale, and a significant change in the frequency of access to backup data.

In the absence of clear guidelines in the regulation, here are some steps that should advance an organization's position as it relates to GDPR storage and backups.

Data mapping Ensure you know where GDPR affected data is stored. Apply a mapping process to get an understanding of where data is stored and how long it is retained. Understand where and what types of data you manage that is affected by GDPR.

Data protection assessment
- Do we comply with data security and encryption?
- Do we comply with recoverability and DR?

Data purge functionality Application teams need to supply logical "forget me" purge programs / jobs that can be used on objects containing multiple data objects (e.g. VSAM data sets containing multiple customer records.) Applications must be enhanced and business logic developed to delete data on customer demand. This should be complemented with proper infrastructure support to do the same for backup copies and archived data.

Backup / recovery processes
- Make required changes to deal with the right to be forgotten in context of restore/recall.
- Implement backup tools with the ability to supply required compliance capability.

When it comes to the tools for running storage backups and archiving on mainframes, here are some questions and requirements to raise with vendors:
- End-to-end encryption
- Role based authorization controls
- Centralized management, Policy-driven automation
- Identify personal data across all copies and locations
- Alert when restoring/recalling personal data
- Quickly search, restore and delete data
- Audit and reporting

And when looking at primary and secondary storage, make sure you have:
- Sufficient capacity for backup frequency to meet RPO
- Redundancy
- Access in DR situations
- Encryption
- Immutability for highly sensitive data
- Support for bare-metal recovery

Summary

The GDPR clearly carries with it backup and archive implications for mainframe. We've listed the challenges, steps to compliance, and the requirements relating to processes and to tools that need to be in place to address these implications.

Model9 is an example of a modern data management software for z/OS that provides standard backup/restore, migrate/archive and recall functions, full volume dumps and space management operations, and implements the requirements relating to GDPR mentioned in this article.

You can listen to more on this in our recent IBM Systems Magazine webinar

Disclaimer

This white paper is a commentary on the GDPR, as Microsoft interprets it, as of the date of publication. We've spent a lot of time with GDPR and like to think we've been thoughtful about its intent and meaning. But the application of GDPR is highly fact-specific, and not all aspects and interpretations of GDPR are well-settled. As a result, this white paper is provided for informational purposes only and should not be relied upon as legal advice or to determine how GDPR might apply to you and your organization. We encourage you to work with a legally qualified professional to discuss GDPR, how it applies specifically to your organization, and how best to ensure compliance. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS WHITE PAPER. This white paper is provided "as-is". Information and views expressed in this white paper, including URL and other Internet website references, may change without notice. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this white paper for your internal, reference purposes only. Published May 2017 Version 1.0