Quest | Metalogix
Now part of Quest

GDPR 101

DEMYSTIFYING
THE EU GENERAL
DATA PROTECTION
REGULATION

Abstract

Technology is redefining the security landscape.

With content being delivered in the cloud and on-premises, organizations are at risk of users exposing sensitive personal and business information. Whether you're part of a global enterprise or an SMB, collaboration in the era of the Modern Workplace is becoming increasingly more reliant on secure data protection.

This eBook will dive into how the GDPR directly addresses the modern challenges of data protection and will propose security best practices that can help organizations comply with the new regulation.

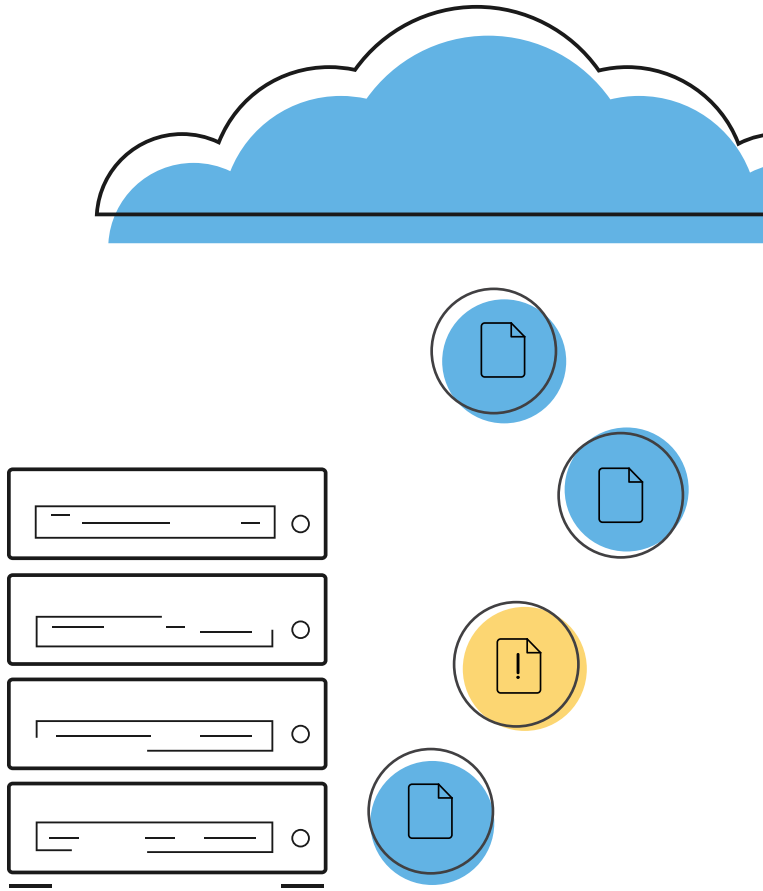


Table of Contents

Quest | Metalogix Now part of Quest

Foreword

"Over the last 12 months, I've had dozens of discussions with customers and partners about their responsibilities in kickstarting GDPR-focused projects and initiatives. The general consensus? IT departments awaited signals from the executive team, budgets weren't discussed with finance, legal departments weren't interested in evaluating IT solutions, and only a few organizations even cared about end-user adoption.

GDPR is changing the way we're thinking about data protection and how we collaborate--regardless if you're on SharePoint, Office 365, or any other collaboration platform.

Ultimately, it's not about check marking the compliance box. It's about protecting the organization from data breaches, penalties, contract terminations, lengthy government audits, and dissatisfied customers.

We all need to change how we think about data protection on a daily basis. Let's start today!"

Ragnar Heil,
Microsoft MVP & Alliances Manager

The Most Important Change in Data Privacy in 20 Years

The EU GDPR, which stands for the European General Data Protection Regulation, is considered the most important change in data privacy since 1998. But the real question is: **Why?**

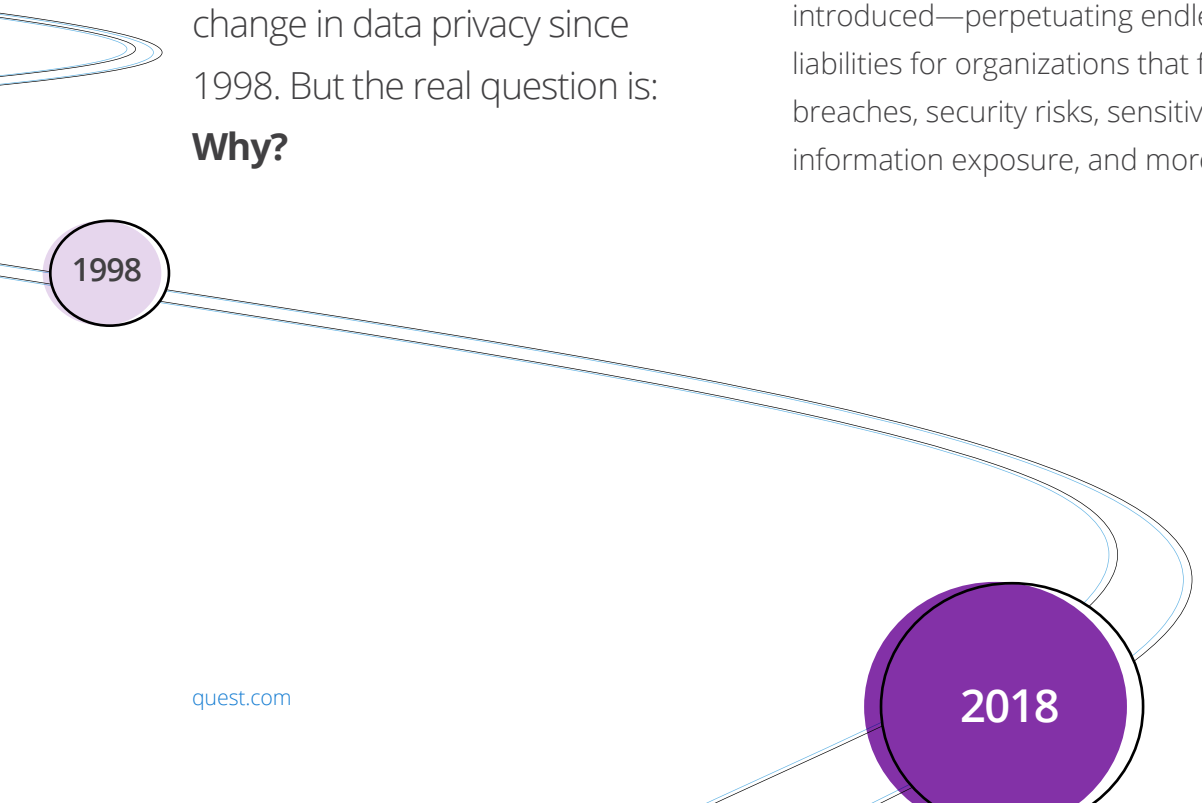
The digital compliance landscape has evolved quite significantly since pre-Y2K. Specifically, the Data Protection Act of 1998 did not account for most of the factors that the Modern Workplace introduced—perpetuating endless liabilities for organizations that face data breaches, security risks, sensitive information exposure, and more.

As a response to the looming threat of cybersecurity risks, the GDPR poses a new set of industry regulations that aim to:

1. Protect EU citizens from privacy and data breaches.

2. Secure EU citizens' personal information that is consumed on any digital platform.

3. Provide EU citizens with a measure of control over their personal information.



Quest | Metalogix
Now part of Quest

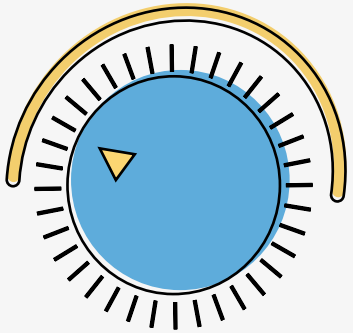
Before you disregard the EU GDPR because: (a) you're not a EU citizen, (b) your organization is not centered in the EU, or (c) your customer base is outside of the EU, it's crucial to note that the legislation applies to EU citizen data that is captured, processed, or stored anywhere.

In other words, if your organization has captured data of an EU citizen at any point, it is subject to GDPR stipulations—no holds barred.

77% of businesses plan to spend $1M+ on GDPR compliance.

92% of U.S.-based multinational corporations claim that GDPR is one of their top data protection priorities.

100% of all surveyed organizations state that enhancing information security is a top GDPR initiative.*



Do you know if your organization processes or stores sensitive information, like Personally Identifiable Information (PII) of a EU citizen?

Locate personal data, assess compliance risk, and safeguard sensitive information with ControlPoint and Sensitive Content Manager.

Quest | Metalogix Now part of Quest

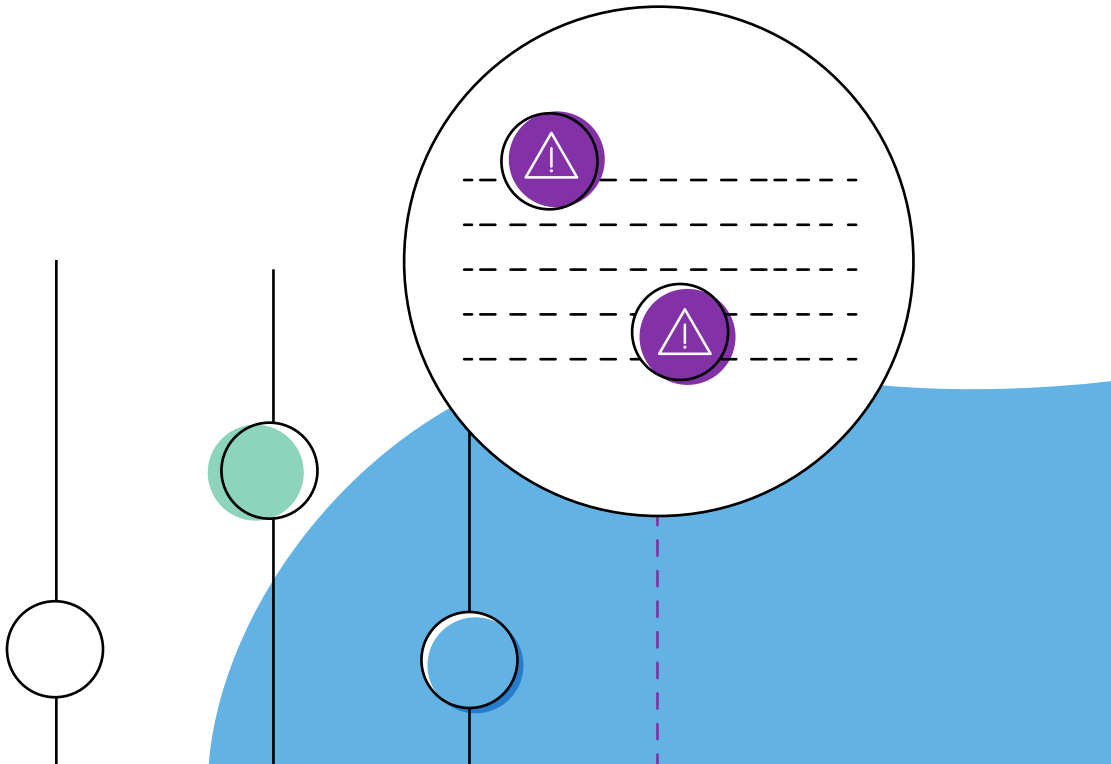
What is the EU GDPR?

As we dive into the EU GDPR, we need to first unpack which areas of data collection and processing are at risk.

Article 4 of the GDPR legislation defines personal data as "any information relating to an identified or identifiable natural person… who can be identified, directly or indirectly, by reference to an identifier."

There are certainly many variances of the word "identify" in that definition, but what this really means is that information such as location data, cookies, and IP addresses are all considered personal data.

In that regard, sensitive (as well as non-sensitive) personal data is subject to GDPR compliance.



From a 30,000-foot view, the data that the GDPR holds liable is classified as:

Sensitive Personal Data

Identifiable data relating to the subject's personal and sensitive information.

Medical: Information pertaining to the data subject's history of medical prescriptions.

Financial: Information related to the data subject's interactions with a bank.

Digital: Information that enables video and information software to recognize the data subject.

Biometric: Fingerprints, facial recognition, retinal scans, and other genetic forms of data.

Emotional: Information related to a data subject's state of mind.

Non-Sensitive Personal Data

Information about the data subject that cannot be used to perpetuate an illegal activity.

Net worth: Proprietary value of items owned, including property, vehicles, commodities, etc.

Services: Automotive services, content services, etc.

Recorded meetings: Information and context around where the data subject is referenced.

Call logs: Where and when calls are made and received from a data subject's phone.

Natural Data

Identifiable and identified data relating to the physical traits of the data subject.

- **Appearance:** Height, weight, hair and eye color, etc.
- **Social:** Profession, function, or organization.
- **Medical history:** X-rays, MRIs, lab results, etc.
- **Connectivity:** IP addresses, cookies, mobile device IDs, etc.

Pseudonymous Data

Data that has been subjected to technological measures.

- **Demographics:** Data collected about the data subject without identifying the subject.
- **Statistical data:** Population information.
- **Additional data:** Any data collected relating to the subject without the subject's identity.

Special Categories

Data that is not collected unless the data collector and processor fall into specific exception groups.

- **Health:** Information related to the data subject's health.
- **Personal convictions:** Beliefs, political opinion, religion, etc.
- **Sexual orientation**

Countdown to the GDPR

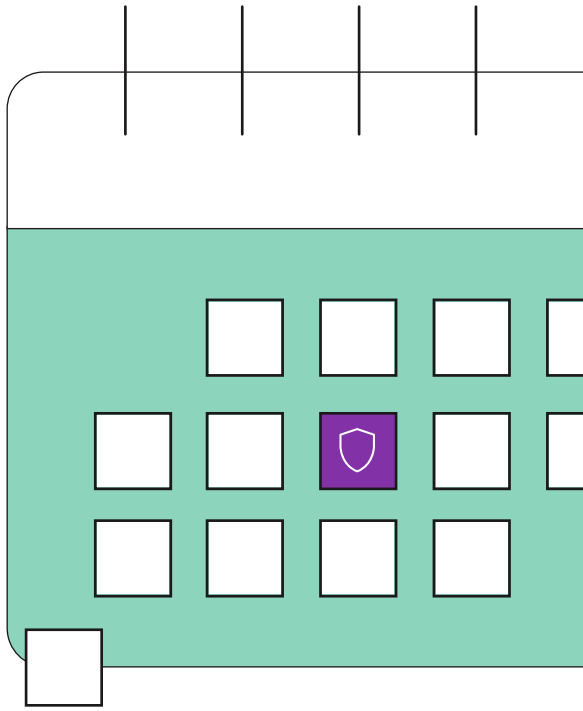
The official GDPR enforcement date was May 25, 2018.

The implementation requires renewed compliance and information governance strategies that address major changes how organizations collect, manage, and store their data.

Though many organizations are still without a clear and concise information security plan, failure to comply with the regulation beyond the enforcement date can (and will) result in harsh penalties and fines.

Penalties & Fines

- Fines of up to 4% of annual turnover or €20 million (~$25M).
- Fines can take a tiered approach, in that an organization can be fined a percentage of the total penalty for not having their records in order.
- Fines apply to both data controllers and processors.
- Fines apply to all electronic storage mechanisms and applications (i.e. Storing content in the "cloud" does not make you exempt).



Quest | Metalogix Now part of Quest

GDPR Key Players

Who controls the data? What happens to the data? How do I respond to GDPR?

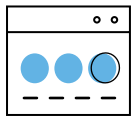
Questions like these are asked on a regular basis, but in order to answer them, we need to dissect how the GDPR affects data within organizations.

Organizations not only need to maintain control over their data, they need to also ensure that third-party access is not granted access to sensitive content by enabling encryption from both endpoints.

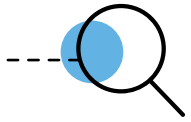
Why? If and when your organization is uninvolved with data collecting or processing, outside vendors (like cloud access security brokers) cannot divulge the data keys.

To better understand how GDPR impacts organizations, let's break down its key players:

Data Subjects



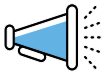
Data Controllers



Data Processors

Data Subjects

Data subjects are citizens of the member states of the European Union, and the legislation applies specifically to them. As such, data subjects are susceptible to stipulations and rights within the GDPR, such as:



Breach Notification

In the event of data breach, and when it is likely to "result in a risk of the rights and freedoms of the individual," the data subject must be notified within 72 hours.

Data Portability

The data subject must receive the data consumed by the data controller in a commonly used, machine-readable format, and has the rights to transfer the data to other data controllers.

Right to Access

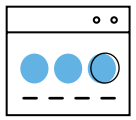
The data subject may inquire whether or not their personal data has been processed, including when, how, and for what purpose.

Right to Be Forgotten

The data subject can instruct the data controller to erase all traces of personal data, extending out to data that has been handed over to third parties.

Right to Object

The data subject may object to the processing (and use) of their data at any time.



Data Controllers

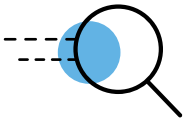
Data controllers include organizations or individuals consuming data subject information.

Historically, data controllers were required to notify Data Protection Authorities (DPA) of their data processing activities, but under the GDPR, they are no longer required to submit data to DPAs. Instead, they can internally maintain records via the appointment of a Data Protection Officer (DPO).

The appointment of a DPO is only required should the data controller require continuous monitoring of data subjects on a large scale, or in the event that special categories could lead to criminal offenses.

Under these conditions, data controllers service the data subjects, in that they are subject to providing personal information when requested. The GDPR also stipulates that the system should be designed in such a manner that it holds and processes data that is absolutely necessary for the interaction between data controllers and data subjects.

For organizations that are categorized as public authorities or deal with large scale systematic monitoring and processing of sensitive personal data, they must appoint a DPO.

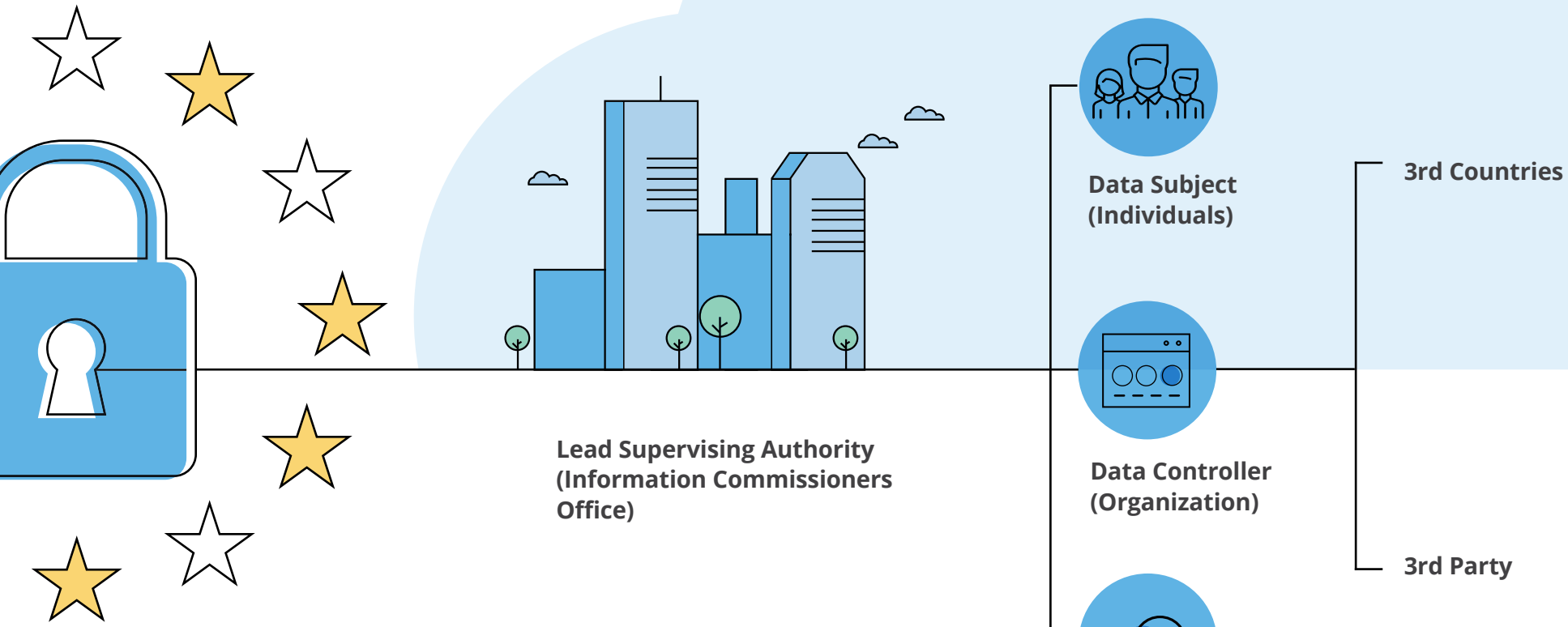


Data Processors

Data processors include organizations that process data collected by data controllers.

Applicable to content in any form, a well-defined records and information management program becomes increasingly more critical when complying with the GDPR. Therefore, data processors impact records management in that they are expected to keep an immutable trail of processing activities and consult data subjects around all aspects of their data, even when in the custody of third-party service providers or contractors.

In other words, even if your organization employs a third-party business to process data collected by your organization, it does not absolve your data controllers of their obligations to service the data subjects. The data processors help bridge and facilitate the relationship between all involved parties by informing the organization of requests to retain, surface, or delete personal information.


European Data Protection Board
Lead Supervising Authority (Information Commissioners Office)
Data Subject (Individuals)
Data Controller (Organization)
Data Processor
3rd Countries
3rd Party

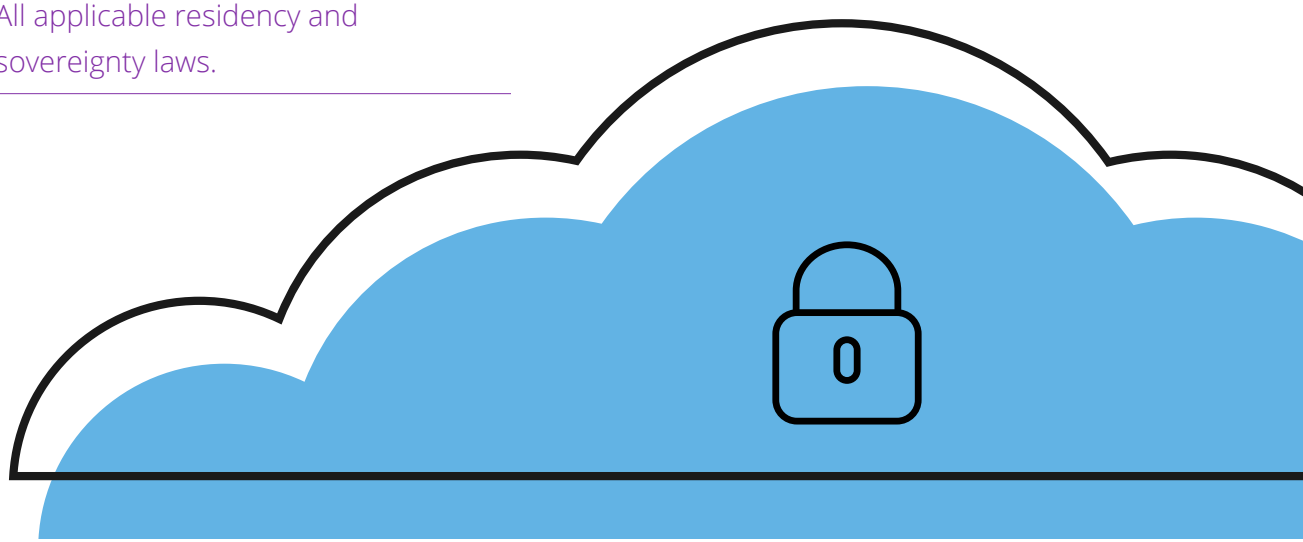
What Happens to Data in the Cloud?

Data governance, sovereignty, and residency are concepts that have been around since before the internet. But with the advent of the cloud and adoption of cloud software like Microsoft Office 365, data is now frequently stored outside state or country borders, which can pose serious ramifications around how local data residency and sovereignty laws could infringe boundaries set by the GDPR.

As such, organizations that utilize cloud services (like Office 365 or OneDrive) that store data outside state or country borders of the data controller or processor should be aware of:

- Sensitive data stored in their data centers.
- All applicable residency and sovereignty laws.

In these cases, the organization will have to apply the necessary security policies to ensure that data is not at risk, encrypt data at rest and in transit, and inform the data subject that their personal information may exist outside their country of residence.



Data Repatriation

Cross-border operations and data flows impact the legality of enforcing GDPR based on data sovereignty laws. A possible consequence of the restrictions of data transfers is that data may be required to be moved back into the country of origin.

As a result, certain member states are already restricting organizations from exporting personal data outside of the EU. Organizations should be aware of this possibility and ensure that they plan for repatriating data, should the state enforce the regulation.

Additionally, organizations that conduct business change projects will need to proactively monitor and change their data storage and transmission components.

"Data controllers need to implement the appropriate technical and organizational measures... in an effective way."

Uncovering Legislative Caveats

Nevertheless, there are caveats in GDPR legislation.

The EU GDPR provides member states with the ability to modify specific articles based on their individual requirements. Therefore, organizations transacting with EU citizens may adhere to multiple forms of the GDPR, based on the member state's interpretation of the legislation.

Does the GDPR Apply to Information Stored in SharePoint?

SharePoint is the market leading content management service, leveraged by over 300,000 organizations worldwide to improve collaboration and manage informational assets. Designed as an intranet and content management portal, this platform supports the modern workforce, making available information wherever and whenever it is needed.

SharePoint is often used to store mission critical business data, ranging from intellectual property and confidential strategic research to documents containing Personally Identifiable Information (PII) about their customers, partners, and employees.

Under the GDPR, organizations will be under enormous pressure to govern sensitive data housed in SharePoint in both legacy and production systems. Organizations must ensure that personal data is identified, managed, and protected in accordance with the regulation, or risk considerable harm to the organization.

Over 50% of information stored in SharePoint repositories is considered "confidential"

Quest | Metalogix Now part of Quest

How Will GDPR Impact Industry Verticals?

Many industry verticals have interpreted GDPR based on their specific business policies, data flows, and capture and extraction processes. Though each industry entails specific processes that will need to be modified to accommodate the legalities of GDPR, the DPO must always ensure regulatory compliance.

Here are a few examples of how industries will need adapt to GDPR and adjust the way they interact with their customers.

Financial

Since financial institutions offer ancillary services to its customers, they will be held responsible for all third-party data management.

They will also need to know where their customer data is stored at all times, as well as how it is stored and what risks they could incur.

Healthcare

For healthcare industries, genetic and biometric data will now be subject to a higher standard of protection.

The processing of these forms of personal data will be prohibited unless certain conditions are met.

Hospitality

The hospitality industry will have to outline its guidelines for collecting and managing personal information.

They must provide a comprehensive account of why they need to process personal data and how long they plan to store it.

Creative

Marketing organizations that engage with third-party vendors to track users and collect data will be responsible for data security and breaches of their data processors' applications.

Agencies will have to develop campaigns to acquire customers while sharing data subject information with partner companies.

Technology

UX and UI organizations will have to build interfaces that adhere to the data capture, erasure, and consent principles stipulated by GDPR.

They will also have to provide varied levels of granularity to users—catering for consent at different stages of processing.

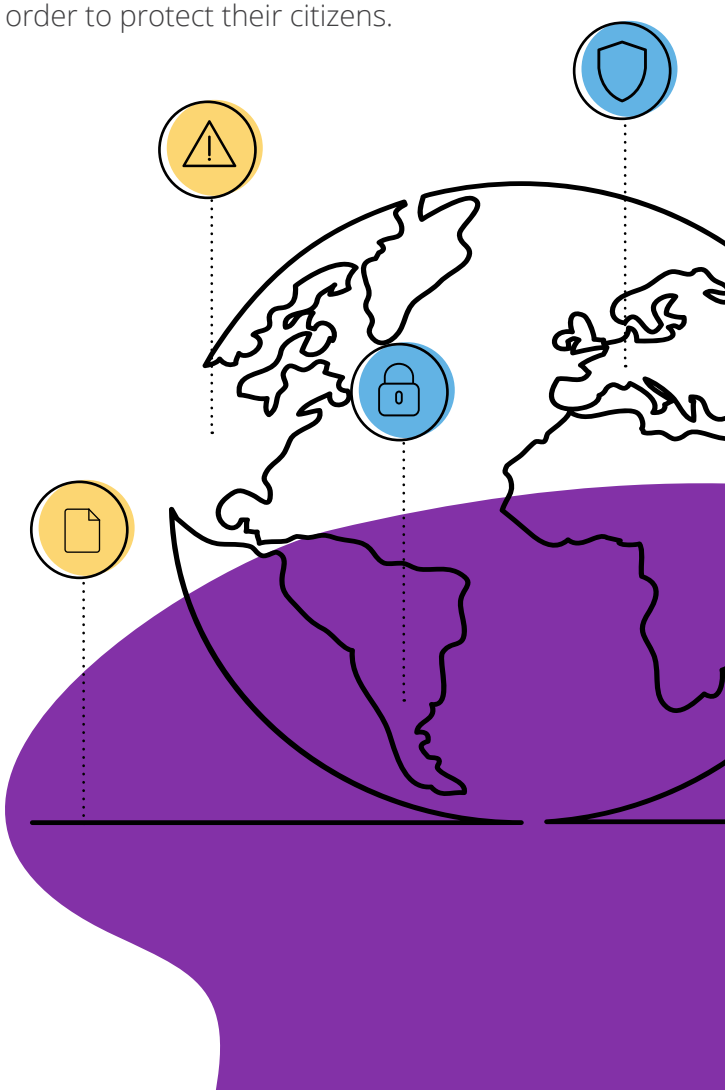
Conclusion

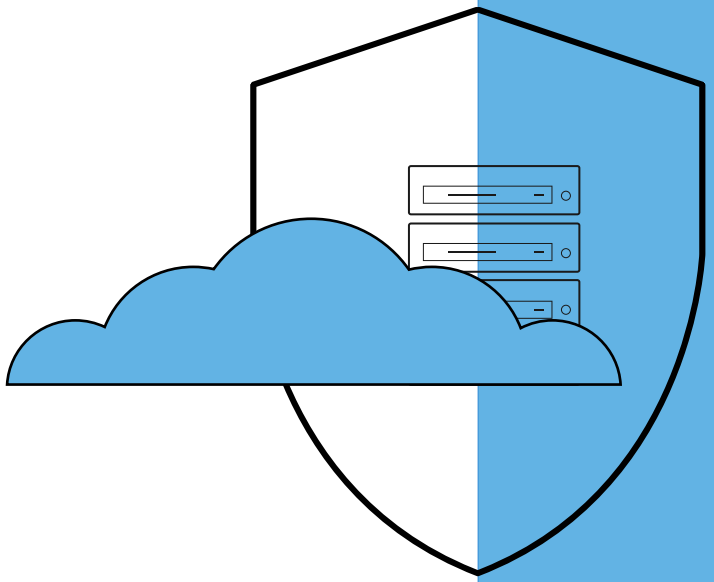
The EU GDPR has far reaching implications to every industry that engages in the practice of capturing, processing, and storing data from EU citizens. As a result, organizations must adhere to the legislation set out by GDPR or face harsh penalties and fines.

The European Union has gone to great lengths to ensure that the privacy of their citizens is maintained. Consequently, not only are data collectors responsible for the data they collect, but also for the information that their data processors manage.

As a result, the EU has provided its citizens with the safety in knowing that they are ultimately in control of what data is collected, how long the data is stored for, who has access to their data, and that they have the ability to erase their data. This is by far the most impactful piece of regulatory legislation pertaining to personal data that has been passed by any country in the world.

The success of the GDPR will see other countries follow suit and institute data protection legislation of their own in order to protect their citizens.





Your GDPR Solutions Suite

GDPR compliance requires a multi-layered approach to secure personal and sensitive data. Whether your journey to GDPR compliance entails a clear plan for legacy systems, hybrid environments, on-premise instances, or the cloud, Metalogix can help you locate, manage, and protect personal data.

Metalogix is a proud Microsoft partner, offering a suite of solutions designed to enhance the capabilities of SharePoint and Office 365.

For more information on how Metalogix can help you address the most challenging aspects of GDPR compliance, check out our GDPR solutions or schedule a live demo with our team of experts!

Quest | Metalogix Now part of Quest

About Metalogix

Metalogix's award-winning cloud, hybrid, and on-premises solutions provide organizations with the freedom and control to migrate, manage, and protect content within enterprise collaboration platforms. Over 20,000 clients trust Metalogix to optimize the availability, performance, and security of their content across the collaboration lifecycle.

Quest provides software solutions for the rapidly-changing world of enterprise IT. We help simplify the challenges caused by data explosion, cloud expansion, hybrid datacenters, security threats and regulatory requirements. Our portfolio includes solutions for database management, data protection, unified endpoint management, identity and access management and Microsoft platform management. *For more information about the Metalogix integration, please visit www.quest.com/quest-acquires-metalogix.*

Credits

Alistair Pugin, Microsoft MVP

Ragnar Heil, Microsoft MVP

Jason Lee, Metalogix

Kristina Benetyte, Metalogix

Shane Bair, Metalogix

Quest | Metalogix
Now part of Quest

References

- https://www.eugdpr.org/
- https://gdpr-info.eu/
- http://www.microsoft.com/GDPR
- * https://www.pwc.com/us/en/increasing-it-effectiveness/publications/gdpr-readiness.html