GDPR – The New Driver for Good Information Governance

Published on Alvarez & Marsal (https://www.alvarezandmarsal.com)

"Information is the oil of the 21st century" [1] and organizations are amassing and storing more than ever before. According to the Gartner group, data is growing 40–60% year on year. For enterprises to successfully manage this exponential growth of information – they must first understand what data they have across the enterprise and how it will affect their operations. Gaining that knowledge is the first step toward developing an information governance strategy that will extract more value from data and minimize the costs and risks associated with managing it.

One of the major new drivers for implementing a strong information governance framework is the European Union's General Data Protection Regulation (GDPR) that comes into effect in May 2018. If organisations do not comply they can face fines of up to €20M or 4% of the undertaking's total worldwide annual revenue (whichever is greater). GDPR will have a major effect on how companies collect and process personal information pertaining to EU individuals. But its reach goes well beyond the borders of the member states (including soon to become ex–member states) – it will be felt globally. Any entity that stores or processes the personal data of an EU individual will be obliged to conform to the new law, regardless of where they reside, or face the consequences.

The upcoming GDPR introduces many new rules and strengthens existing requirements which must be actively managed, covering a wide range of areas such as: the right to be forgotten / right to erasure; privacy impact assessments; breach notification; data protection by design and default; the right to data access; the right to data portability and 'consent' / 'explicit consent' of the use of personal data. These will cause significant challenges for all departments involved and the systems that service them. Teams that work with customer data and 3rd parties need to understand their responsibility and accountability as either the controller or processor.

According to Jonathan Kirsop, a Partner at Stephenson Harwood, "One of the biggest changes in the GDPR is the introduction of the so–called 'accountability principle'. Effectively, this shifts the burden of proof onto controllers (and processors) to be able to demonstrate privacy compliance through accurate and comprehensive record keeping and policies. With regulators enjoying much enhanced rights of audit, this principle creates added incentive on organisations to introduce effective information governance structures and manage the information held".An effective information governance strategy is the key weapon in a company's arsenal to address these data requirements. To be successful, an information governance program should develop and implement the processes, policies, procedures and controls to manage information at an enterprise level. This includes the ability to support the immediate and future regulatory, legal, risk and operational needs.

One of the biggest challenges companies face in implementing an information governance framework resides in unstructured data (data created by employees / clients, e.g., emails, word documents, presentations, etc.). According to reports from IDC, Forrester and Gartner, approximately 80% of enterprises' storage footprints consist of unstructured file data. Additionally, in a survey that was performed by the Compliance and Governance Oversight Council (CGOC), around 70% of data retained inside an organisation has no business value and no legal or compliance obligation.[2]

The reality is that over time a company's data ends up as unmanaged dark content in data silos. Much of it is redundant, obsolete or trivial (ROT) data and has no business value and should have been defensibly deleted. Instead the data lies dormant in a multitude of repositories – often being duplicated, replicated and copied increasing the operational costs. In addition, it often loses context, ownership or critical information around the original value or purpose of the information – thereby the organization can lose the ability to make valid business decisions. This dark data can also contain personally identifiable information (PII), and presents a cyber–security nightmare which is now regulated under the GDPR.

So why are organisations still retaining this excess data? The need and use of information during its lifecycle falls under the contrasting requirements of various business stakeholders: legal, records management, compliance, privacy and security, IT and/or individual business units. Whilst the stakeholders are able to coordinate and comply with disparate needs, rules and regulations, the ultimate ownership of data is defaulted to IT which is unable to make a decision on its retention as this requires an insight into the operational business context. Typically, this results in a "keep everything forever" mind–set across the business.

Organisations should use the opportunity of what the GDPR is enforcing to redefine information governance – aligning key stakeholders, processes, policies and procedures to business requirements and systems. By taking this holistic view of information governance, organisations are able to gain visibility into their entire data estate and accept that not all information is of equal value and risk. This approach results in turning the huge amount of data held into available, usable and relevant information assets – improving business intelligence and employee efficiency. Furthermore, the organisation will be in a far better position to assess risk, security or compliance exposures, and IT can expect to see substantial reductions in costs through storage optimization and operational efficiencies.

Where do we start?

In most cases, achieving an information governance "utopia" within organisations appears unattainable and often the most difficult question to answer is "Where do we start?" Initially, the key is for the organisation to perform a current state assessment of its information governance maturity against an industry best practice. The level at which the organisations sits in an information governance maturity model defines how extensive the pathway for improvement needs to be. The maturity levels range from limited and chaotic through to a fully mature and optimised process. Having this initial assessment means that a set of initiatives can be established to move the organisation to its desired end state. Initial initiatives typically include:

- **Seek legal advice and update policies** in order to comply with the ever changing regulatory environment.
- **Establish a Data Governance Council** consisting of the key stakeholders with 'C' level sponsorship to ensure that an information governance program has the authority required to implement the necessary change – both from an organisational and IT perspective.
- **Build a data map**. A data map is an information inventory that allows an organisation to understand exactly what data it holds, why they are holding it, where does it reside and how is it being managed. This is a fundamental requirement for an organisation to respond to an individual's GDPR request.
- **Perform data privacy impact assessments**. Define and reduce the privacy risks identified within processes and systems.
- **Perform data assessments on high risk systems**. As previously stated much of an organisations data resides in dark data repositories with a potential to contain personally identifiable information, sensitive and highly confidential information that creates a massive risk to the organisation that needs to be quantified and remediated.
- **Define an information governance framework** appropriate for the organisation's needs.

The evolution of technology has revolutionised how organisations perform business, resulting in the exponential growth of data, the majority without context or value. The growing awareness of the risk associated with this data and its' potential for public damage is driving the revolution on regulations – the GDPR putting the individual's data rights above the needs of an organisation. Therefore, a robust information governance strategy is required to marry the data requirements and business processes with the ever changing regulatory and technological landscape.

[1] Peter Sondergaard, SVP Gartner, Gartner Symposium/ITxpo, 2011.

[2] CGOC, Summit 2013 Survey, 2013.

Source URL: https://www.alvarezandmarsal.com/insights/gdpr-new-driver-good-information-governance

Links
[1] https://www.alvarezandmarsal.com/insights/gdpr-new-driver-good-information-governance

Authors:
Phil Beckett, pbeckett@alvarezandmarsal.com, +44 207 663 0778