GDPR and the Impact on Data Archiving and Information Governance

smarsh™

Contents

Introduction: GDPR in the Context of Today's Business

The General Data Protection Regulation (GDPR) has been voted into law by the European Union (EU) and went into effect on 25 May 2018. However, while this data protection and privacy legislation is enacted by the European Union, it will have far-reaching consequences for firms doing business with EU citizens around the world.

Banks in Australia count EU nationals among their account holders; surgeons in the United States cater to patients from the United Kingdom (UK). Even after the UK leaves the EU, the UK government has indicated that the principles of the new regulation will be adopted by local legislature. In essence, any organisation holding data on EU nationals will need to comply with the new regulation, regardless of where the organisation is based.

The GDPR replaces the Data Protection Directive, which was enacted in 1995, before social media, instant messaging, and other collaborative applications became entrenched in day-to-day business. The GDPR looks to close that gap to protect the privacy and security of data collected by organisations on individuals with today's communications tools.

The GDPR should also be seen against the wider context of high profile data breaches which businesses from banking and finance, to healthcare, and telecommunications have suffered in recent years. These data breaches have ranged from the deployment of ransomware, malicious insider activity, or most commonly, the loss of data through the lack of oversight of employee activities and inadequate procedures and training[1].

In an environment where businesses are implementing more communications and social channels in the workplace, the risk of a data breach is at a heightened level. Clearly, organisations need to urgently review their technology, practices and processes to prepare for GDPR. Organisations that fail to comply with the regulation can be fined up to $20 million, or 4% of the organisation's global revenues - a cost that makes the GDPR impossible to ignore.

Keep Calm and Carry On?

The time to take GDPR seriously is now. A recent survey of organisations that need to comply with the guidelines set forth in the GDPR showed that the majority of respondents (57 percent) said discussions regarding the allocation of additional resources - headcount, budget or other - had begun, but no decisions have yet been made. A further 23 percent said no additional resources will be made available for GDPR compliance[2].

One of the first steps organisations preparing to comply with GDPR can do is to assess what the new guidelines mean for the way data is held and processed within the business; how and which employees and departments have access to the data; and what sort of training and procedures are in place.

And as many organisations now employ technology and service providers to collect, process and store data, they must be increasingly diligent in ensuring that their service providers are equipped to address GDPR demands. Organisations need to evaluate which service providers embrace privacy by design versus those who approach privacy as an afterthought.

Key Principles of the GDPR

For organisations preparing to comply with the GDPR, Article 5 outlines the key data privacy principles to be followed:

- Personal data should be processed fairly and transparently by organisations
- The use of any data collected must be specific, explicit and legitimate
- Use of the data should be limited to the purpose for which the data was requested
- Organisations need to reasonably ensure that personal data is accurate and up to date
- Personal data should not be stored for longer than necessary
- Personal data needs to be secured and organisations should take steps to insure against accidental loss, destruction or damage

Enshrining the rights of individuals

Articles 15-22 of the GDPR also provides the following rights for individuals:

- The right to be informed about how the data that they provide will be used
- The right of access to their personal data and how it is processed
- The right to rectification if the data held is inaccurate or incomplete (including instances where data has been disclosed to third parties)
- The right to erasure - or 'the right to be forgotten' - individuals can request that their personal data be deleted
- The right to restrict processing - where just enough information about an individual is held but not processed
- The right to data portability so individuals can obtain and reuse their personal data for their own purposes across different services
- The right to object to processing in the form of profiling for instance, direct marketing and processing for purposes of scientific/historical research and statistics.

Demonstrating compliance

Article 25 of GDPR specifies that companies are expected to demonstrate that they have addressed "Data Protection by Design and Default". This means that organisations will need to invest in technology, processes and training to secure and manage personal data. This also requires that organisations undergo regular third party audits to ensure that controls are enforced, and can submit this evidence to the regulator upon request.

Notification of breaches

Under Article 33 of the GDPR guidelines, organisations have a responsibility to report data breaches to relevant supervisory authorities within 72 hours of the organisation becoming aware of it. If the breach is sufficiently serious, the organisation should also notify the public. Failure to report breaches could result in a significant fine up to 10 million Euros or 2 percent of an organisation's global turnover.

Restrictions on transfer of personal data

Articles 44-50 of the GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations. Personal data may only be transferred outside of the EU where the European Commission has decided that a third country, a territory or one or more specific sectors in the third country, or an international organisation will provide an adequate level of protection to the personal data comparable to the provisions made under the GDPR.

The Implications of the GDPR for Data Archiving and Information Governance

The importance of GDPR to the data archiving and information governance market is that it makes it clear that compliance is more than checking a box. GDPR elevates the importance of data privacy as a critical element to consider when selecting one solution over another - ensuring that it is built to meet an increasingly complex set of global data protection requirements. This is particularly important for archiving or governance services that are delivered via cloud services providers, whose operational and data security practices vary widely.

Here are 5 actions for organisations to implement today:

1. **Understand and Segment by Data Location:** Organisations need to understand where personal data collected from individuals in the EU resides and the potential risks it is exposed to. Under GDPR Article 15, EU citizens have the right to enquire if and how their data is being processed. For organisations to be able to do this, they must first understand where the personal data of that individual is stored.

   For instance, an organisation may store personal data of EU citizens through cloud-based services. Under the GDPR, organisations will need to understand whether that data is stored within an EU or US data center location. They should also confirm that data is exclusively stored in that location as some cloud services providers distribute data across data centers for technical reasons such as load balancing or resource optimisation.

   Once confirming data location, companies can implement the appropriate retention and disposition policies that comply with GDPR guidelines.

   Maintaining European data in the EU (or partnering with firms who have this capability) is another option to comply with privacy regulations. When dealing with matters that include data sets from the EU, hosting the data locally and limiting access to specific GDPR-trained staff for review is a viable and commonly used option. Firms with European data centers can often offer the additional benefits of knowledge and experience navigating country-specific data privacy regulations if data needs to be transferred elsewhere, for instance, to the US.

2. **Understand, Limit and Supervise Employee Access to Personal Data:** For organisations to be able to meet new GDPR guidelines that enable individuals to request to see how their data is being processed and request for processing to be limited, they need to understand and limit which of their employees have access to personal data. Those who do, need to be trained, and there should be documented procedures for handling personal data.

   It will also simplify compliance if organisations are able to segregate access to that data so that only employees in designated roles or locations can access data from customers who are based in the EU. In a multinational corporation, for example, a legal team that needs to access data from EU-based users for eDiscovery purposes, should only be granted access if they have been trained to process data to GDPR standards.

3. **Assess Existing Capabilities to Search, Filter and Retrieve Data Quickly:** The GDPR means that organisations need to assess if existing methods and procedures can comply with the new data privacy requirements. For instance, organisations will have less time to comply to a request by an individual for the "right to access" their data. Organisations will have to respond to requests without delay and within one month of receipt of the request. They must have the ability to hone in on relevant data, filtering personal information not pertinent to the topic being litigated or investigated. Furthermore, organisations will have to provide this information for free (a fee can be charged if the request is deemed to be too complex but this cannot exceed the administrative cost of performing the task).

4. **Ability to Delete Complete Records for Individuals:** One of the "rights" in Article 17 of the GDPR, is the "right to erasure," otherwise known as the right for an individual to be "forgotten." This means that organisations need to be prepared to receive requests from individuals for their personal data to be deleted within a company's systems.

   A recent study found that 90 percent of businesses think it will be hard for them to delete customer data if they receive such a request, and only 40 percent of companies have a system in place that allows them to do so[3].

   Addressing this requirement means that organisations need to be able to perform selective disposition, where an individual's personal data can be found and extracted from the organisation's content store.

5. **Auditing and Reviewing Suppliers:** Article 25 of GDPR also explicitly calls for an obligation for organisations to implement technical and organisational measures to demonstrate how data protection has been integrated into their processing activities. One way that organisations can determine this is to be satisfied that suppliers who handle or process personal data are able to provide assurances that data is secured, and data governance can be proven.

   This could mean examining the provenance of technology and service providers to ensure they can prove that their solution complies with globally-recognised standards, such as the ISO27000 Information Security Management, ISO27018 Cloud Privacy Protection, or the Statement on Standards for Attestation Engagements (SSAE-16) auditing standard.

How Smarsh Can Help

Since 2001, Smarsh has been helping organisations get ahead – and stay ahead – of the risk within their electronic communications. With innovative capture, archiving and monitoring solutions that extend across the industry's widest breadth of channels, customers can leverage the productivity benefits of email, social media, mobile/text messaging, instant messaging/collaboration, websites and voice while efficiently strengthening their compliance, recordkeeping and e-discovery initiatives. Smarsh helps organisations meet requirements outlined within GDPR in several important areas:

1. **Privacy by Design and Default (Article 25):** Ensuring that data is properly protected is a core component of the Smarsh Connected Archive, including defined processes, procedures and training on data privacy protection contained within the following audited attestations:

   - SSAE-16 SOC2
   - ISO 27002
   - HIPAA (Health Insurance Portability and Accountability Act)
   - ISO 27018 Cloud Privacy Attestation

   The ISO2700 attestation specifically ensures that Smarsh:

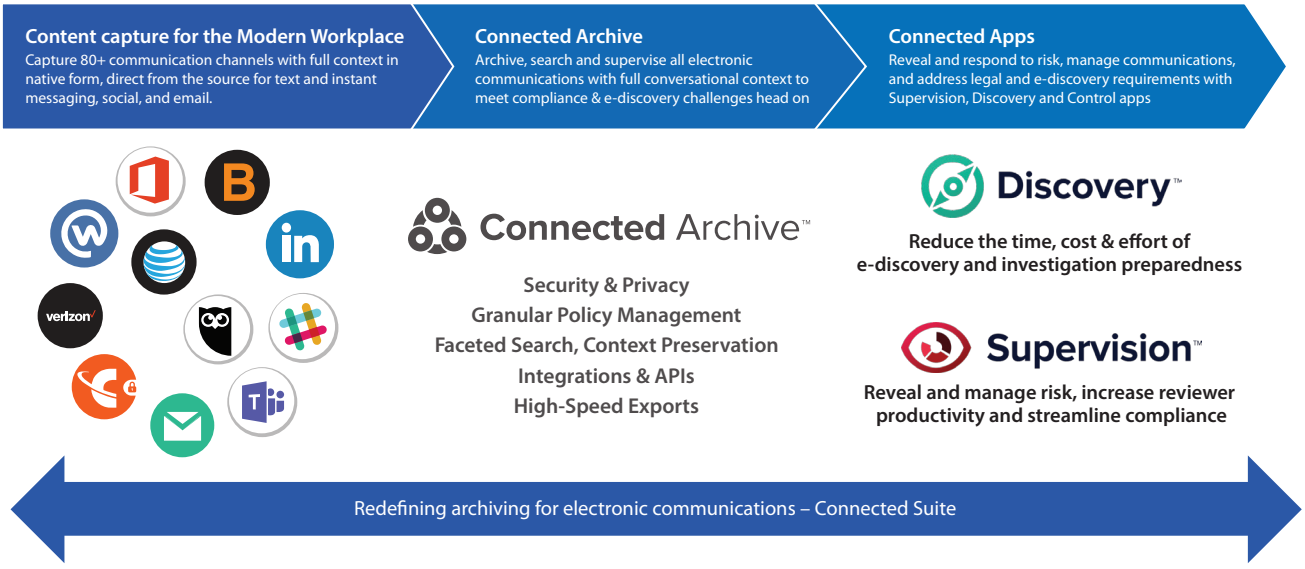
   - Systematically examines the organization's information security risks, taking account of the threats, vulnerabilities, and impacts;
   - Designs and implements a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (e.g., risk avoidance or risk transfer) to address those risks that are deemed unacceptable;
   - Adopts an over-arching management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis.

   Additionally, security of personal data is provided through the use technologies and defined and audited processes for advanced data encryption, authentication, key management, datacenter security, network security, application security, storage security, system monitoring, and on-going security assessments.

2. **Right of Data Access (Article 15):** In this area, EU citizens have the right to enquire if and how their data is being processed. Addressing this right first requires an understanding of where of that individual is stored. Unlike other cloud archiving providers, Smarsh stores data within an EU or US data center location – and does not distribute data across center for technological reasons (e.g. load balancing or resource optimization). Additionally, for those with strict data locality requirements, data can be archived locally or in an on-premises instance in partnership with IBM SoftLayer.

   With data location being easily identifiable, companies can easily govern data to ensure that applicable retention and disposition policies can be defined and implemented specific to each geographic region. Organisations can also segregate access to that data so that only designated roles or locations can access data from specific users. For example, those who are responsible for performing e-discovery can be granted access to data from EU-based users only if they are knowledgeable of GDPR requirements.

GDPR places a higher premium on data privacy protection and good information governance practices that have been designed into the Smarsh Connected Suite from the start – not only for email, but over 80+ communications channels. This, combined with the ability to quickly search and retrieve EU citizen's data, are key reasons why multi-national firms doing business with EU citizens should consider Smarsh.



Learn more about retention and supervision solutions of electronic communications for FCA regulated firms

Regulatory compliance - including voice capture
Preserve and store data on tamper-proof media to meet FCA and MiFID II requirements.

On-demand production and trade reconstruction
Securely export data for further legal or regulatory review. Reconstruct communications around a specific trade.

Exam tested
ocate and retrieve electronic communications quickly, and be prepared for regulatory examinations with on-demand data production.

Audit trail for compliance
Show proof of supervisory procedures through a detailed audit history of every action taken in the platform.

Compliance workflow
Customize supervision policies and keyword lists and streamline compliance review workflow.

Administration and migration
Whether you're a 1-person firm or have 1000s of branches, it's easy to manage users and to migrate data.

Visit www.smarsh.com/FCA-regulated-firms

1 "The UK's 15 most infamous data breaches", Tech World, John E Dunn, Nov 18, 2016, http://www.techworld.com/security/uks-most-infamous-data-breaches-2016-3604586/

2 "UK Businesses are not ready for GDPR", IT Pro, Jane MacCallion, 2 Jun 2016, http://www.itpro.co.uk/it-legislation/26658/uk-businesses-are-not-ready-for-gdpr

3 "90% of businesses think it's too hard to delete customer data", IT Pro, Clare Hopping, 19 Oct 2016, http://www.itpro.co.uk/data-protection/27428/90-of-businesses-think-its-too-hard-to-delete-customer-data

Additional Resources

For organisations that are active in the EU, whatever size and type of business, there is no time to lose. Don't waste any time to put proper systems and processes in place, or your organisation may become vulnerable to non-compliance with GDPR.

To learn more about how Smarsh can help your organisation prepare for GDPR call +44 (0) 800 048 8612 or click here to find out more about The Archiving Platform, watch our solution in action, and access other resources.

+44 (0) 800-048-8612 www.smarsh.com @SmarshInc SmarshInc Company/smarsh