Three Keys to Your GDPR Compliance Strategy

Focus on Unstructured Content, Metadata and the User

Outside Europe, government regulations tied to the protection and security of individual information has had a relatively low profile. That's about to change.

The amount of personal data stored by companies and governments has soared, and the value of that data has multiplied as more and more personal business is transacted on the internet. Identity theft has become a major new crime. In addition to the disruption to business and the impact on customer loyalty that data breaches create, many jurisdictions are looking to bring their data protection legislation into line with the new, internet-based world – although unfortunately, not in line with each other.

A new set of European rules and standards related to privacy and data protection (the General Data Protection Regulation, or GDPR) has set in motion a mad compliance scramble not only for European companies, *but for any company doing business in Europe or with European customers*. The regulation codifies many privacy rights and creates an explicit obligation to the controller as well as the processor to be able to demonstrate their compliance to the GDPR. The clock is ticking – the regulation goes into effect in May next year, and the potential penalties for non-compliance are significant (up to 4% of the total worldwide annual turnover).

It is important for non-European companies to remember that the old escape clauses for non-European companies no longer work. Non-European companies utilized "Safe Harbor" provisions to comply with the original data protection regulation. Safe Harbor Privacy Principles were developed between 1998-2000 and in July 2000, the European Commission (EC) decided that US companies complying with the principles and registering that they met EU requirements could transfer data from the EU to the US. The international Safe Harbor Privacy Principles were overturned on October 24, 2015 by the European Court of Justice after a customer complained that his Facebook data was insufficiently protected.

According to the Digital Clarity Group, "The GDPR could be a mortal threat to your company's existence — and it makes fundamental decisions about data collection, processing, and storage into key strategic business issues. An adequate response requires C-level (and even board-level) attention and involvement immediately."

But where should you start? I would suggest you start with:

- Unstructured Content
- Metadata
- The User

1 Unstructured Content.

Managing unstructured information and documents are key to GDPR compliance. According to the European Commission, “Personal data is any information relating to an individual, whether it relates to his or her private, professional or public life.” The Commission notes, “It can be anything from a name, a home address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer’s IP address.”

Companies must be able to identify any place or document containing personally identifiable information (PII) and be able provide an index of that PII data to the customer if requested. They must also be able to protect information in transit, provide a right (and proof) of erasure, correction and portability, and be able to prove enforcement of records management policies and practices. All of the above are impossible in an organization of any scale without a comprehensive Enterprise Information Governance system that is able to ingest or migrate content, extract information and the associated metadata from corporate records, classify, enrich, protect, preserve, share and control the entire set of information, company-wide.

2 Metadata.

There are two ways of looking at metadata in the context of GDPR.

The first way is that effective metadata management is obviously key to automating the governance tasks required by the GDPR. A key element in GDPR is data security. A metadata driven system can easily enforce advanced security (dynamic security based on the value of the metadata) to protect the content based on what is it and not on where it is stored. Deloitte notes, “Insight is only possible with metadata management. You need to be able to extract the needed insights from your data. This is only possible with proper metadata management. If you know which personal data you process, and the properties of processing, using the right tooling, you can get the insights you need.”

The second way is to understand that metadata itself – if potentially linked to personally identifiable information – is subject to GDPR. Advanced metadata extraction and management can be used to identify and re-tag Personally Identifiable Information (PII) and to add value to otherwise unsearchable content. Consider the following from Steve Kenny at IAPP: “…any data used to make inferences linked tenuously or otherwise to a living person is personal data under GDPR. Cookie IDs, IP addresses, any device identifier? All personal data. Even metadata with no obvious identifier is caught under the GDPR's definition of personal data.”

This dichotomy is reflected in the clash between past practices of data *maximization* – “Let’s gather as much data as possible since storage is cheap and hope that someday we can find value in it” – and the GDPR requirement for data *minimization* – and obligation to only gather that information that is necessary, for the shortest time possible.

3 The End User -- a comprehensive GDPR solution should address not only C-Level Compliance and Security Executives and Legal Directors, but every single line of business user working with Personally Identifiable Information (PII).

The concept of Privacy by *Design* is critical in structuring end user GDPR roles and responsibilities:

According to EU Data Protection Regulation, “…privacy by design means that each new service or business process that makes use of personal data must take the protection of such data into consideration. An organisation needs to be able to show that they have adequate security in place and that compliance is monitored. In practice this means that an IT department must take privacy into account during the whole life cycle of the system or process development.”

Per Phillip Mahan, Director of the Office of the CPO at Ionic Security, Privacy by Design principles include the following:

1. **Proactive not Reactive; Preventative not Remedial** -- Controllers must assess risks presented by processing activities and develop and implement adequate measures to address these risks.
2. **Privacy as the DEFAULT** -- Personal data must be protected without action from the individual. GDPR has specific requirements to ensure the data subject does not have to take action in order for their data to be protected.
3. **Privacy Embedded into the Design** -- Privacy Controls should be embedded in the architecture of IT systems, operations, and business processes without lessening functionality for the User.
4. **Full Functionality: Positive-Sum non-Zero-Sum** -- It is possible to have Privacy AND Security. This principle seeks to accommodate all legitimate interests and objectives in a ‘win-win’ manner, not in a way that encourages trade-offs.
5. **End-to-End Security: Lifecycle Protection** -- Embed Privacy and Data Protection into your systems throughout the data lifecycle from collection to destruction.
6. **Visibility and Transparency** -- Assure all stakeholders that you are operating according to stated promises and objectives subject to independent verification.
7. **Respect for User Privacy** -- The purpose for the GDPR is the protection of personal data for the citizens of the European Union. The EU Charter states that Privacy is a fundamental Human right.

This means that your entire GDPR strategy – from definition to design to implementation to operation – must include clear processes and procedures at the operating level. This includes clear roles and responsibilities, training, and regular review and audit cycles.

This Tip Sheet is sponsored by Star Storage.

Star Storage is a global technology provider developing and delivering state-of-the-art information protection and management solutions for top private and public organizations. With 16 years of experience, own Intellectual Property and a portfolio of over 500 customers on 4 continents, with strong expertise in top industries such as banking, insurance, telecom, manufacturing, utilities and public administration, the company plays a key role in the digital transformation, mobile and cloud journey of any size organization.

You might also be interested in:

- Creating the Simple Enterprise (white paper)
- Why Mobile Makes the Difference (Infographic and White Paper)
- Redefining Technology: The Tool—Not the Goal (white paper)
- 6 Shortcuts to Tear Away the Paper (Infographic)

AIIM (www.aiim.org) AIIM is the global community of information professionals. We provide the education, research and certification that information professionals need to manage and share information assets in an era of mobile, social, cloud and big data.

AIIM
1100 Wayne Avenue, Suite 1100
Silver Spring, MD 20910
+1 301.587.8202
www.aiim.org

AIIM Europe
Broomhall Business Centre, Broomhall Lane,
Worcester, WR5 2NT, UK
+44 (0)1905 727600
www.aiim.eu