Is the GDPR the New EU Version of SOX?

In today's constantly shifting digital climate, governments across the globe are working around the clock to strengthen and unify data protection for citizens and organizations alike. In alignment with global trends, the European Parliament, the Council of the European Union and the European Commission have all come together to establish the General Data Protection Regulation (GDPR).

The intention behind the GDPR is to return power over personal data back to EU citizens and residents while also simplifying the regulatory environment for the international business community by harmonizing data protection regulations throughout the EU by addressing the export of personal data outside of the EU.

While compliance requirements are varied throughout the law's text, they can be grouped into the following themes:

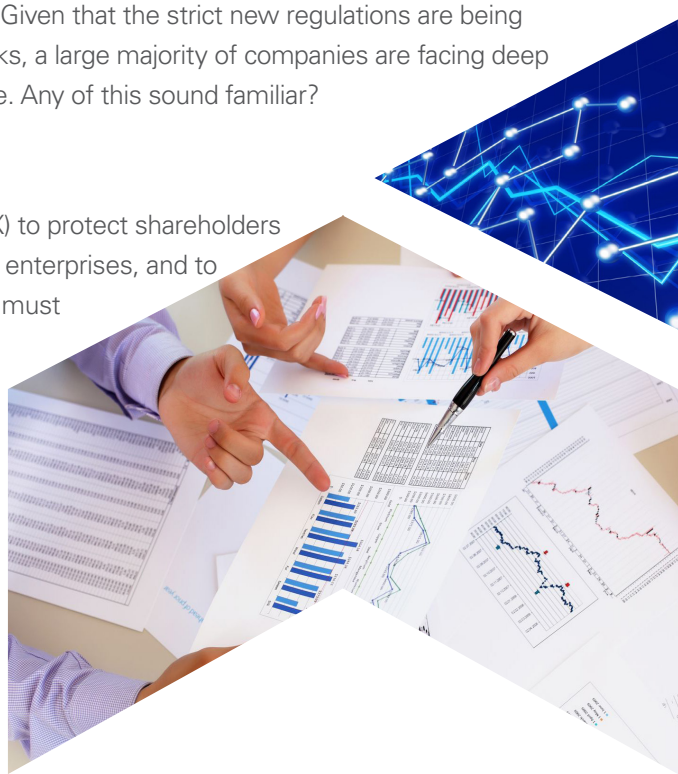
- Data Control & Security
- Right to Erasure
- Due Diligence & Risk Mitigation
- Breach Notifications

The GDPR was adopted on April 27, 2016 but comes into effect May 25, 2018 after a two-year transition period where it was being integrated to replace the current data protection directive (Officially Directive 95/46/EC) of 1995.

Despite the two-year transition period, the GDPR is sure to create unique challenges for organizations throughout the world doing business with the EU before, during and after the May 25 deadline. Given that the strict new regulations are being imposed on all types and sizes of companies and come with hefty fine risks, a large majority of companies are facing deep concerns surrounding whether or not the requirements will be met in time. Any of this sound familiar?

The Sox Parallel

In 2002, the United States Congress passed the Sarbanes-Oxley Act (SOX) to protect shareholders and the general public from accounting errors and fraudulent practices in enterprises, and to improve the accuracy of corporate disclosures. All public companies now must comply with SOX, both on the financial side and on the IT side.



While the act does not specify how a business should store records or establish a set of business practices, it does define which records should be stored and the length of time for the storage.

To comply with SOX, corporations have been required to save all business records, including electronic records and electronic messages for a minimum of five years.

Advaion

In nearly direct alignment to SOX, the GDPR is imposed unilaterally for application in the EU only, but due to the size of the market, will impact organizations internationally, as so many have operations in the EU. And being less familiar with data privacy practices prevailing in Europe, non-EU companies may find the GDPR to be even more concerning than the introduction of SOX 2002 find it maybe even more concerning, as shown by the current multiplication of conferences on the topic in the U.S. alone.

In short, CFOs are more concerned than ever given the costs associated with putting the necessary processes and resources place to respond to compliance requirements. Mitigating the costs of compliance ever since the "SOX wave" has already proven to be incredibly challenging. It's no surprise many are bracing for the realities of a similar scenario with the advent of GDPR.

Still, Improved Technologies are making a Difference

The good news? There is a silver lining. Technologies have come a long way since the early days of SOX.

GDPR is also very much about documenting, making sure that the needed policies, controls, and procedures are in place, and being able to demonstrate this to the authorities. When it comes to governance, organizations can capitalize on years of experience learning things the hard way by having to document and manipulate mass quantities of spreadsheets, Word documents and multiple other files, while also having to tie together mounds of information for reporting, certifications and sign-offs. Having survived the governance fires of SOX, companies should be able to create a less costly, more efficient and effective path to compliance.

Obviously, new and improved supporting technologies that are available to manage such compliance requirements will help. These could include:

- A robust control framework
- Complete policy lifecycle management
- Control evaluation and monitoring capabilities
- Comprehensive reporting features

A number of vendors have emerged in response to new compliance requirements at a diverse level of depth, which means unlike the confusion accompanied by the early days of SOX, organizations have various, superior-quality technologies they can use to govern their GDPR compliance, allowing CFOs and executive boards throughout the globe to rest a little easier, knowing their reporting efforts are in good technological hands.

About Advaion

Advaion is an innovative consulting firm that was founded by former Big 4 Accounting Firm personnel with national and international expertise across a wide range of industries. Our solutions are focused on three main segments: Accounting, Technology and Management ("ATM").

For more information on collaborating with Advaion on your GDPR Compliance, please contact our Compliance Leaders:

Advaion

Pavan Satyaketu
646 240 4771 ext. 201
psatyaketu@advaion.com

Garth Stewart
954 889 3407 ext. 202
gstewart@advaion.com

advaion.com