

GDPR Compliance & Requirements

Key Challenges & Opportunities

When the General Data Protection Regulation (GDPR) entered into the public consciousness last year, it became a boogeyman for non-compliant businesses handling EU citizens' personal data, regardless of the company's physical location. Who can blame them for being scared? Hefty fines threaten companies that don't comply with the GDPR's very stringent requirements on data management, storage, usage and security. The GDPR also expands the definition of "personal data" to include people who can be indirectly identified through factors like location or browser cookies, and the regulations set new limits on how, why and for how long data can be held and processed.

By now, you should already be aware that your company must meet GDPR software requirements by May 25, 2018. There's no denying that reaching full compliance for data privacy and risk management within this timeline poses many key challenges. However, if you view these challenges as opportunities to optimize your business, you are already on the right path to operating more safely and more efficiently to gain an edge on the competition. Here are three key areas where your company can leverage risk and turn potential liabilities into tangible assets.

LEVERAGE COMPLIANCE OPERATIONS TO ESTABLISH YOUR REPUTATION AS A LEADER IN RISK MANAGEMENT

In light of the Equifax data breach that left up to 143 million Americans at risk of identity theft, following closely on the heels of similar breaches at Yahoo, Target and others, corporate data practices are undergoing more scrutiny than ever before. For an unprepared company, the spectre of a potential public relations and organizational brand disaster due to GDPR non-compliance or a data breach is enough to cause cold sweats. The cost of a damaged reputation is likely to exceed any potential fines by a large margin.

But for a responsible business that has already established a solid compliance framework and thorough risk-assessment processes, GDPR presents a new opportunity to build trust with customers and establish your company as an industry expert. As users and customers grow increasingly savvy about the importance of their personal data, it's not enough to simply react to incidents with a high-paid damage control team.

To truly establish your company as a trustworthy data steward, your customer base will expect to see proactive data controls in place that help limit exposure and avoid incidents. These controls also mean that in the event of a data incident, your team will be prepared to fully understand the extent of the issue, accurately communicate with regulators and limit any potential fallout by demonstrating to customers and the public that you are in control of the situation. While the avoidance of fines and negative news cycles is a strong motivator, the true prize for GDPR compliance (and risk management in general) is a pristine reputation that eliminates one more barrier between your company and its next major deal.

THE BENEFITS OF KNOWING YOUR DATA FRAMEWORK EXTEND BEYOND COMPLIANCE

Increased cyber threats and digital risk have moved IT security talk into the boardrooms. In the past few years, senior leadership teams across many different companies have become far more attuned to data security and risk management. The fate of their businesses often rest on technical, IT-related decisions. It makes sense that companies will be better positioned for success with a clear idea of how data is captured, classified or segmented, where it is stored and how it's secured. A universal map of your data streamlines workflows and offers a better understanding of how your business operates, so you can make more informed decisions. Some processes that your team needs to follow in order to build this data map - and meet GDPR compliance - include:

- Developing or procuring a risk assessment process and registry to log and manage potential data management and security issues
- Updating and distributing customer agreements to meet transparency and purpose requirements
- Upgrading or replacing enterprise hardware and operating systems to support modern data-encryption standards

A better understanding of your data structure also mitigates vendor risk. It eliminates uncertainty and allows you to responsibly contract third-party products or software with peace of mind. Under the GDPR 2018 regulations, a data breach allowed by a third-party vendor places liability on both the vendor and the business that ultimately owns the data. However, the business can avoid liability by proving it had

implemented requisite safeguards to help prevent an issue.

GDPR COMPLIANCE WILL COST YOU MONEY - ARE YOU INVESTING WISELY?

Do you need to be compliant with EU GDPR? Potential fines of €20 million, or 4 percent of global annual revenue - whichever is greater - says the answer is "yes." But meeting GDPR software requirements is not just a chance to avoid fees. It's also an opportunity to invest in a more secure future, where your business can leverage risk mitigation to drive innovation, inform savvy business decisions and capture a competitive advantage.

One of the key requirements of GDPR 2018 is appointing a Data Protection Officer (DPO) whose core activities consist of processing operations that require regular and systematic monitoring of data subjects on a large scale. Investing in a data expert can help your company stay several steps ahead of the regulatory curve while streamlining your data resources and operations. This appointment can also help to promote a company-wide culture that understands and respects the importance of data protection, from the ground floor to the penthouse boardroom.

While potentially costly, building security into your products and implementing breach-notification processes guarantee better-protected businesses and customers. These types of vital infrastructure investments help prevent financial waste due to non-compliance fees and also greatly improve the operation of your business.

SAI GLOBAL CAN HELP YOU ACHIEVE COMPREHENSIVE GDPR COMPLIANCE

GDPR 2018 levies a number of strict regulations regarding the access and sharing of EU customer data, including security regulations on products and operations. But these demands also present huge opportunities to build trust with your customers and become a more responsive, confident business. SAI Global recognizes the difficulty in preparing for GDPR 2018. The Digital Manager 360 platform works to eliminate data chaos, reduce risk and drive smarter decisions. Digital Manager 360 automates the entire IT GRC management process and provides a flexible, out-of-the-box software platform that can be configured to and integrated with existing environments, technologies and processes for immediate benefits and return on investment. Learn more about this powerful, user-friendly platform by downloading the brochure [here](#).

Find out more

CONTACT US

[SAI Global Homepage](#) > [Risk & Compliance](#) > [Digital Risk Software](#) > [GDPR Compliance And Requirements - Three Key Challenges and Opportunities](#)

Risk & Compliance

Compliance Risk
Digital Risk
Information Security Training
Ethics & Compliance Learning
Operational Risk
EHS Risk
Vendor Risk
Business Continuity

News & Resources

SAI Global Newsroom
Blog
Upcoming Events
Case Studies

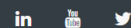
About Us

Company Overview
Careers
Contact Us

More Solutions

Assurance
Standards
Property
SAI Global Group

[Accessibility](#) [Terms & Conditions](#) [Privacy Policy](#) [Data Subject Requests](#)



©2019 SAI Global Pty Limited, ABN 67 050 611 642