GDPR compliance in a data-driven world

Insights from a 2018 survey
Compliance doesn’t have to be a scary word, even when facing the multifaceted challenges of the European Union’s General Data Protection Regulation. In fact, following through with plans for sustainable GDPR compliance can have many long-term benefits for your organization. That’s because relying on data-driven decisions across the board sets you on track to gain a competitive edge.

In February 2018, SAS conducted a survey with 183 global, cross-industry businesspeople involved with GDPR at their organizations. Based on the survey results, this e-book delves into the biggest challenges and opportunities organizations have faced on the road to GDPR compliance.

Read on for advice from industry experts about the best path to compliance. Learn what steps your peers across a variety of industries have already taken, and discover how an integrated approach from SAS can continue to guide your journey toward GDPR compliance.
Basic tenets of the GDPR

Who it affects, why and what defines personal data.
The European General Data Protection Regulation elevates the protection of personal data to a top legal compliance and strategic priority for companies around the world that work with the personal data of European residents.

The GDPR defines personal data broadly and puts the individual at the center of data protection. It gives every EU resident the right to know and decide how his or her personal data is being used, stored, protected, transferred and deleted. Individuals have the right to restrict further processing and to request that all their data be erased (the right to be forgotten).

GDPR compliance requires organizations to make a holistic review of their practices regarding the collection, use and protection of potentially enormous amounts of data. As companies take measures to comply, most will experience several challenges along the way.

Why GDPR?
While the GDPR and related topics around data privacy and protection have been in the news for a long time, many organizations are still not sure about their organization’s level of compliance with the GDPR. And financial penalties for noncompliance loom – they range up to €20 million (about US$23 million) or 4 percent of annual global revenue, whichever is greater.

Who does the GDPR affect?
An organization is not exempt from GDPR requirements just because it’s not based in an EU country. This sweeping legislation applies globally for any organization that processes the personal data of individuals who live in the European Union. That could be an employee who lives in Germany but works for a company in New York. Or a customer from Ireland doing an online transaction with a California-based retailer.

Work toward compliance with SAS® for Personal Data Protection
A revised definition of personal data

Personal data, according to the GDPR, is any data that allows for the identification of an individual, directly or indirectly. A variety of factors that can identify a person – IP address or location data, for example – are now considered personally identifiable information and are covered as a way to ensure personal data protection. It’s a broad definition that’s expected to expand over time.

Preparations

The GDPR is designed to ensure continued, stringent protection and enforcement – and to simplify the regulatory environment for global organizations. Concern about the potential for heavy fines pushed many organizations to complete preparations for compliance. For example, our survey shows that 64 percent of organizations have a fully or partially complete GDPR compliance checklist in place. Another 30 percent are making these plans. While only 7 percent of the respondents said they were fully compliant now, 27 percent said they were “almost” compliant.

While heavy fines are a concern, it’s important to remember that the GDPR is designed to ensure continued, stringent protection and enforcement – and to simplify the regulatory environment for global organizations. Concern about the potential for heavy fines pushed many organizations to complete preparations for compliance. For example, our survey shows that 64 percent of organizations have a fully or partially complete GDPR compliance checklist in place. Another 30 percent are making these plans. While only 7 percent of the respondents said they were fully compliant now, 27 percent said they were “almost” compliant.

Implications: IT, business and AI

Despite hefty fines, not everyone is confident that they understand the broad reach and implications of the GDPR. Close to 40 percent of survey respondents either aren’t sure or do not think their organizations fully understand the impact GDPR will have on them. The 2018 survey revealed the most significant effects respondents think GDPR will have on their organizations. For example, 75 percent said GDPR would significantly affect their IT operations, 63 percent said it would significantly affect how they conduct business and 49 percent said GDPR would significantly affect their AI projects. Here are three major ways they felt GDPR would affect their artificial intelligence goals: Establishing informed consent (33 percent), logging/presenting to auditors details on the use of profiling (25 percent), and requiring human involvement in AI decisions (22 percent).

“Changing your perspective to think of the GDPR as an opportunity, not a burden, will not happen overnight. But it’s smart to be proactive,” says Kalliopi Spyridaki, Chief Privacy Strategist at SAS. “Doing so will prepare you for EU laws on data that are following as we move toward a fully regulated data market.

The EU - and many individual EU countries - is currently designing its policies and laws around artificial intelligence. This work includes issues around algorithmic transparency and accountability.

Other EU policy initiatives currently in the pipeline are aimed at regulating data access and data ownership, including in the context of B2B relationships.

It's the perfect time to get a deeper understanding of all your company's data and create a comprehensive data strategy that will carry you well into the future.

The EU - and many individual EU countries - is currently designing its policies and laws around artificial intelligence. This work includes issues around algorithmic transparency and accountability.

Other EU policy initiatives currently in the pipeline are aimed at regulating data access and data ownership, including in the context of B2B relationships.

It's the perfect time to get a deeper understanding of all your company's data and create a comprehensive data strategy that will carry you well into the future.
7% of respondents say they are fully GDPR compliant.

**IMPACT ON AI**

How will GDPR affect artificial intelligence projects?

- Most concerning GDPR requirements:
  - Establishing informed consent.
  - Logging/presenting to auditors details on use of profiling.
  - Requiring human involvement in AI decisions.

49% said GDPR would significantly affect their AI projects.

**COMPLIANCE**

Are you fully GDPR compliant?

- 7% fully compliant
- 8% US organizations fully compliant
- 5% EU organizations fully compliant

Work toward compliance with SAS® for Personal Data Protection
A structured process is critical to compliance

58 percent of organizations have a fully or partially complete process in place.
In working to achieve GDPR compliance, it helps to have a structured process. Of our survey respondents, 58 percent say they have a fully or partially complete structured process in place. Another 35 percent are making plans for a process.

Only 50 percent of our survey respondents agreed that their organizations would be compliant by the GDPR deadline. The others either disagreed or weren’t sure of their compliance status. If you’re not confident about your organization’s compliance readiness, it’s time to evaluate your GDPR compliance checklist and structured process, then make necessary adjustments.

“In the future, data protection compliance becomes more about how well your business processes are organized than formally getting an authorization to process data,” says Olivier Penel, EMEA Data Management Business Director for SAS. “In that perspective the majority of the respondents in the survey still have a long way to go. In order to successfully deploy a structured process for GDPR compliance, it’s mandatory for most companies to have a data protection officer. These professionals understand data privacy and know how to apply the law. Beyond the legal requirements, it’s important that this person understands the value of data as a strategic asset for the business.”

Penel thinks it will pay to have a data protection officer who can inspire change within the organization – not only for the sake of compliance, but also to embed personal data protection and data governance in general as essential business requirements.
Telia Denmark tackles GDPR using SAS® for Personal Data Protection

Telia Denmark, which provides internet, phone and television services, is part of the Telia Company – the fifth-largest telco in Europe. To address GDPR regulations, Telia Denmark used SAS to help it locate and identify personal data across its many legacy data sources.

Under GDPR regulations, companies must be able to document their processes for obtaining and storing personal data – and their ability to identify and extract all personal data related to an individual. To ensure that all personal data is located and identified in its systems, Telia Denmark designed a data discovery process and a set of rule files. This is not as simple as it sounds. For example, a telephone number is a personal identifier, but a telco customer may also be identified in a number of other unique ways, such as through a SIM card number, an IMEI or IMSI number.

Telia Denmark used SAS software to carry out data discovery processes on a large number of separate IT systems that contain personal data. This means the company can live up to GDPR demands of being able to identify and locate personal data within its own systems. So, if a customer calls and wants to exert his or her right to have files deleted, a command to all Telia Denmark systems can be created to ensure that this will happen.
Benefits of the GDPR

Improved data governance is just the beginning
The GDPR is the first change to EU privacy and protection laws in more than 20 years. But companies don’t have to start from scratch as they approach GDPR compliance. Many can assess their current data governance program, determine where the gaps are, then start addressing their gaps.

**Improved data governance, trust and personal data quality**

Data – in constantly growing amounts – is a valuable business asset. The GDPR gives organizations the opportunity to reassess all the data governance policies they’re using. Not only for personal data, but for all data. With the correct governance policies in place, companies can comply while building a competitive advantage. For example, imagine being able to improve analytical processes, optimize operational efficiency and reduce costs.

Our 2018 survey confirmed the many business benefits of GDPR compliance efforts. Of those surveyed, 84 percent said they expected GDPR to improve their data governance. Better data governance was the top anticipated benefit in our 2017 survey as well.

In the 2018 survey, 68 percent said GDPR would positively affect trust between customers and organizations. Additional benefits organizations expect to gain by GDPR compliance are improved personal data quality and enhanced organizational image. Many also expect to move closer to becoming a data-driven organization.

---

**What benefits will GDPR bring to your business?**

- **84%** anticipate GDPR will improve data governance.
- **68%** anticipate GDPR will increase trust.

**More benefits**

- Improved personal data quality.
- Enhanced image.
- Move toward data-driven business.
Be fully GDPR compliant. Strengthen customer relationships and trust.

Interamerican, the largest private insurance company in Greece, provides life, health and property insurance to more than 1 million customers – a vast amount of data to handle and protect. Interamerican used the opportunity presented by GDPR compliance requirements to bolster data protection, build customer trust and retain its loyal customers.

Under its new data governance model, employees operate in a more secure, efficient way. The new GDPR requirements provided an opportunity to invest in and boost the company’s data ecosystem. New tools, expertise and knowledge are used not only to comply with regulations and protect the data, but also to advance data management practices by providing enhanced capabilities for data analysis, data quality and data handling.

Interamerican expands personal data protection with SAS®

“Trust is synonymous with insurance and is the cornerstone to building and keeping long customer relationships. We will promote this extended trust coming out of GDPR compliance, hoping to gain a clear advantage in the Greek insurance market. The GDPR is not just another compliance framework, but a great opportunity to enhance operational excellence.”

Xenophon Liapakis, CIO of Interamerican

Listen to the story
Top challenges of the GDPR
And what you can do to address them
The GDPR makes organizations accountable for personal data protection. They will have the burden of proof when it relates to whether, how and how well they protect personal data. This includes having security measures in place to guard against data breaches, and taking quick action to notify individuals and authorities in the event a breach does occur. And it makes legal compliance an issue that should be at the top of the agenda for companies of all sizes, across sectors.

What are the challenges?
The GDPR gives every EU resident the right to know and decide how their personal data is being used, stored, protected, transferred and deleted. Individuals have the right to restrict further processing and to request that all their data be erased. This brings up questions about the tools, accountability (people) and processes that organizations need to have in place.

Some of the top challenges our survey respondents cited were: Identifying all sources of stored personal data; acquiring the skills to manage GDPR compliance; dealing with consent management; and complying with new requirements on profiling.

What are the biggest challenges of GDPR for businesses?

63% say it will significantly affect how they conduct business.

75% say it will significantly affect IT operations.

More challenges
- Identifying all personal data.
- Acquiring skills to manage compliance.

What are the experts saying?
If you’re ready for a deeper dive, read our blogs to see what GDPR topics the experts are talking about - such as how to:

- Protect structured versus unstructured data.
- Link consent information with data usage policies and personal data.
- Know and prove who requested personal data queries (and when).
- Understand the "black box" of automated decision making.
- Improve customer experience by complying with the new regulation.
5 pillars of the GDPR
Take an integrated approach
It’s clear that noncompliance with the GDPR could be a real threat to the future of many organizations. On the other hand, personal data has tremendous value and can create significant competitive advantage if it’s managed properly. Let’s look at an approach some companies are using to address GDPR requirements (and get a competitive edge).

5 Pillars of GDPR

- **Access**
- **Identify**
- **Govern**
- **Protect**
- **Audit**

To address GDPR compliance, you can’t rely on common knowledge or perception of where you think personal data might be. The regulation requires organizations to prove that they know where personal data is - and where it isn’t. This makes it important to access all your data sources. No matter what the technology - traditional data warehouses and Hadoop clusters, structured and unstructured data, data at rest and data in motion - you must investigate and audit what personal data is being stored and used across your data landscape. Seamless access to all data sources is a prerequisite for building an inventory of personal data so you can evaluate your privacy risk exposure and enforce enterprisewide privacy rules.

Once you’ve got access to all the data sources, you’ll need to identify the personal data that can be found in each. Often, personal data is buried in semistructured fields. You’ll need to be able to parse those fields to extract, categorize and catalog personal data elements such as names, email addresses and Social Security numbers. Considering the volumes of data at hand, this cataloging process can’t be manual. And you not only need to parse and classify personal data - you also have to accommodate varying levels of data quality. Things like pattern recognition, data quality rules and standardization are vital elements of this process.

Work toward compliance with SAS® for Personal Data Protection
Getting a grasp on personal data starts with being able to define what personal data means and then sharing this understanding across your organization. For GDPR, privacy rules must be documented and shared across all lines of business. This is the way to make sure personal data can only be accessed by those with proper rights, based on the nature of the personal data, the rights associated with users groups and the usage context. To achieve this, roles and definitions must be established in a governance model. Then you can link business terms to physical data sources and establish data lineage from the point of creation to the point of consumption. This provides you with the required level of control.

When you’ve established the personal data inventory and governance model, it’s time to set up the correct level of protection for the data. You can use three techniques to protect data:

- **Anonymization**, which removes personally identifiable information from data.
- **Pseudonymization**, which replaces personally identifiable information in data.
- **Encryption**, which encodes personally identifiable information in data.

You must apply the appropriate technique based on the user’s rights and the usage context – without compromising your growing needs for analysis, forecasting, querying and reporting. The easiest way to protect data privacy is actually to press the delete button, keeping only the data you need to run critical business processes and added-value analysis.

Another vital element of GDPR is auditing. At this stage, the regulator will ask you to prove that you:

- Know what personal data you have and where it’s located, across your data landscape.
- Properly manage the process for getting consent from individuals who are involved.
- Track and document how personal data is used, who uses it and for what purpose.
- Have the appropriate processes in place to manage the right to be forgotten, data breach notifications and more.

Implementing the GDPR will affect your entire organization. You’ll need to go back to the drawing board and rethink how personal data is handled from the source to the point of consumption. You’ll also need to consider how your data management and data governance frameworks will support GDPR requirements.

**Integrated approach**

Being able to create detailed reports about personal data usage is not simply a requirement of the GDPR – it helps you manage the risk exposure of your entire organization. Our approach is designed to guide you through these efforts, from gaining access to data sources to auditing the results. What’s more, this approach can strengthen your business, help you create deeper bonds with customers, and spur innovation that could have positive, far-reaching implications for future growth.
Appendix: Summary of survey results
As an analytics and data management software and services provider, SAS has particular interest in the GDPR and the effects it will have on our clients.

Main objective of our research
Understanding the current status of companies’ GDPR readiness and the process through which companies are preparing for GDPR compliancy.

Methodology
An online survey conducted by SAS. Recruitment via targeted marketing emails and several social media channels. Want to learn more about our survey participants? The following charts describe the sizes and industries of respondents’ organizations as well as the GDPR-related roles and overall functions of those individuals who took the survey.

The following charts provide details about survey respondents, including company size, industry, job role and overall job function.

What is your role in preparing your organization for GDPR?

- Overall responsibility for GDPR projects/initiatives in my organization or division: 28%
- Part of the team that manages GDPR projects or initiatives in my organization or division: 46%
- In charge of some GDPR projects or initiatives: 26%
Which of the following best describes your function in the organization?

- Data Privacy Officer: 7%
- Legal/Compliance/Privacy: 8%
- General Management: 18%
- Business Consultant: 11%
- Information Technology: 23%
- Information Security: 3%
- Marketing/Sales: 12%
- Other: 18%

Work toward compliance with SAS® for Personal Data Protection
How many employees work for your organization worldwide?

- Fewer than 50: 33%
- 50 to 249: 14%
- 250 to 999: 16%
- 1,000 to 4,999: 15%
- 5,000 or more: 22%
What best describes your organization's primary industry?

- Banking: 14%
- Education: 11%
- Government: 5%
- Health Care: 9%
- Insurance: 12%
- Communications: 6%
- Services: 19%
- Other: 24%

Work toward compliance with SAS® for Personal Data Protection
Face the multifaceted challenges of GDPR compliance and gain long-term benefits for your organization with SAS® for Personal Data Protection.

Follow us: