# Working toward GDPR compliance

Insights from a SAS survey and an end-to-end approach

sas

Compliance doesn't have to be a scary word – even when facing the multifaceted challenges of meeting the European Union's May 2018 deadline for its General Data Protection Regulation. In fact, charting a course for sustainable GDPR compliance now can have other long-term benefits for your organization. That's because it sets you on track to gain a competitive edge as you learn to rely on data-driven decisions across the board.

In spring 2017, SAS conducted a global GDPR survey among 340 business executives from multiple industries. Based on the results of that survey, this e-book delves into the biggest challenges and opportunities organizations face on the road to GDPR compliance.

Read on for advice from industry experts about how to get started on the best path to compliance. We'll also share the steps that your peers across a variety of industries have already taken, and an integrated, five-step approach from SAS that can help guide your journey to GDPR compliance.

## Table of contents

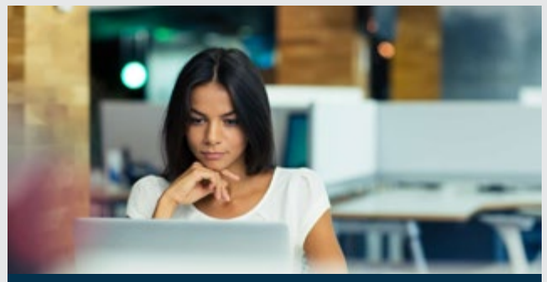


Basic tenets of the GDPR

3

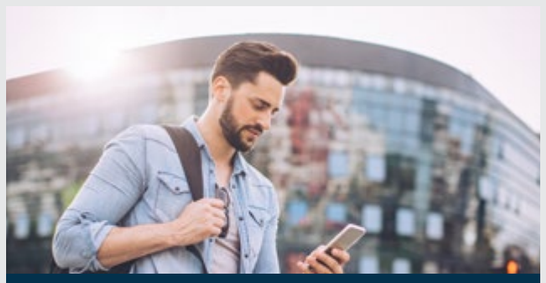
A structured process is critical to compliance

7



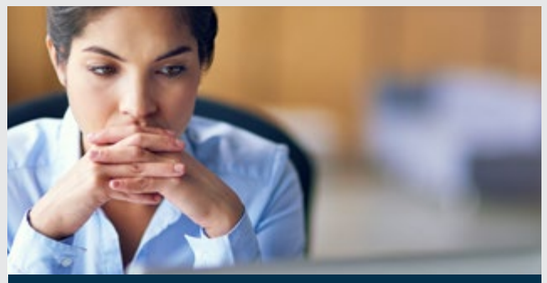
Top 3 benefits of the GDPR

10



Challenges of GDPR compliance

14



5 steps to managing GDPR

17

Appendix: Summary of survey results

20


# Basic tenets of the GDPR

Who it affects, why and what defines personal data

The European General Data Protection Regulation was adopted in April 2016 and will go into effect on May 25, 2018. The GDPR 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, they will likely experience several challenges along the way.

## Why GDPR?

Several data privacy developments have created a lot of hype about the GDPR in recent years. One notable example is the invalidation of Safe Harbor, a mechanism enabling data transfers between the EU and the US that's been replaced by the Privacy Shield. Confronted with a deadline of May 25, 2018, some organizations are getting downright nervous about complying with the GDPR. Especially considering that financial penalties for noncompliance 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.

## 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 covered as a way to ensure personal data protection. It's a broad definition, and one that's expected to expand over time.

**Kalliopi Spyridaki,** Chief Privacy Strategist at SAS.

Watch a video interview with Spyridaki.

*"The new definition of personal data is indicative of the overall tone of the new legislation", says Kalliopi Spyridaki, Chief Privacy Strategist at SAS. "Under the General Data Protection Regulation, personal data is considered a valuable asset. And requirements and obligations around it are tightening up considerably. Not coincidentally, this goes hand in hand with technological trends like cloud computing, big data and the Internet of Things. With each of these technologies, data gathering and adequate data analysis are becoming strategic differentiators. By recognizing this, the GDPR is basically catching up with reality."*

## Deadline

The GDPR is designed to ensure continued, stringent protection and enforcement – and to simplify the regulatory environment for global organizations. As the deadline for compliance approaches, concern about the potential for heavy fines is pushing preparations to the forefront at many organizations. Research shows 56 percent of the organizations surveyed are already taking steps to prepare for GDPR.

## GDPR awareness

Despite hefty fines, not everyone is aware of the actual reach and implications of the GDPR. Our research shows that fewer than 50 percent of the respondents are convinced their organizations fully understand the impact GDPR will have. In general, large organizations are more aware of GDPR and its implications than smaller organizations. Regarding industries, only 26% of government organizations are fully aware of the impact, compared to 56% of telco, media & communication organizations. In general, awareness is at 42 percent across other industries.

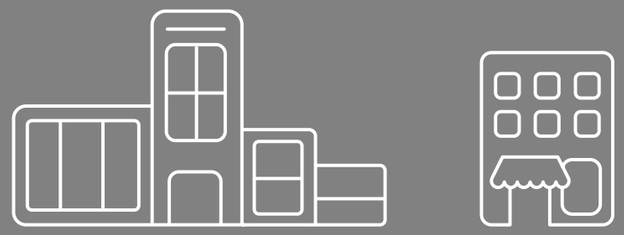
**56%**

of organizations are already taking steps to prepare for GDPR

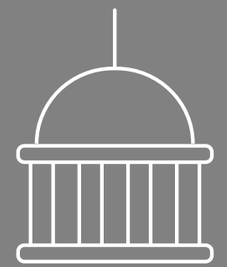
## **Question:** Is your organization fully aware of the impact of GDPR?

| Percentage of "yes" responses by industry. | Total | Financial services | Telco, media & communication | Government & health care | Chemical & manufacturing | IT & services |
|---|---|---|---|---|---|---|
| | **42%** | 47% | 56% | 26% | 43% | 42% |

## Key takeaways



Most respondents feel that GDPR will have a big impact on their organizations. However, many respondents (58 percent) indicate that their organizations are not fully aware. Large organizations do somewhat better than small organizations. They are better prepared and better informed about GDPR implications.



Government organizations are least aware of the impact of GDPR.

67% of large organizations (over 5,000 employees) are already taking the necessary steps to prepare for GDPR, compared to 47% of small organizations.

54% of large organizations are fully aware of the impact of GDPR, compared to 37% of small organizations.

Only 26% of government organizations are aware, compared to 42% across industries

# A structured process is critical to compliance

But only 45% of organizations are taking that approach

To achieve compliance in a timely manner, organizations need to have a structured process in place. Unfortunately, the research shows that this is not the case for 55 percent of the respondents. Of the 45 percent of organizations that do have a process planned, almost 80 percent have already started their journey to GDPR compliance. And 66 percent of the respondents who have a structured process in place believe they will meet the GDPR deadline of May 2018.

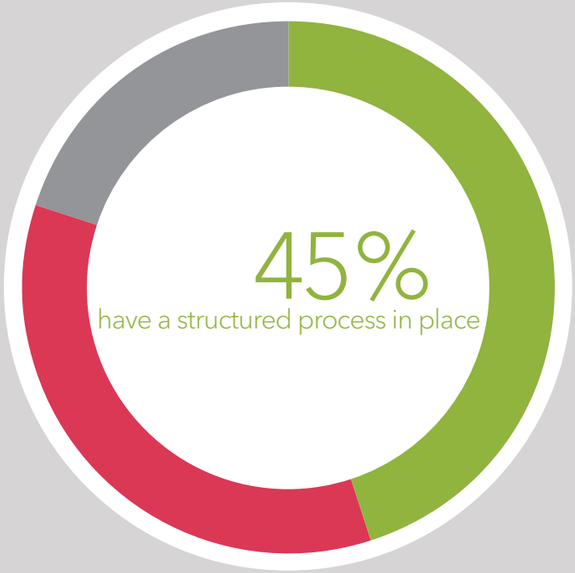
If your organization is among the 55 percent that doesn't have a process in place, or has a process but hasn't begun to implement it, it's imperative that you begin the journey to GDPR compliance as soon as possible. May 2018 will be here sooner than you think.

"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.

## Only 45 percent of organizations have a structured process in place to comply with GDPR

Large organizations do much better than small organizations; 60 percent of large organizations have a structured process in place. There are no significant differences between industries.




## Of this 45 percent, only 66 percent think that this process will lead to successful compliance

This is related to the fact that some people do not know how to determine when they are GDPR compliant.


## Only 24 percent of organizations make use of external consulting to become GDPR compliant

The organizations that have a structured process in place use external consulting more often (34 percent) to comply with GDPR.


In this video interview, Olivier Penel, EMEA Data Management Business Director for SAS, shares his advice on how to comply with GDPR

# Top 3 benefits of the GDPR

Improved data governance is just the beginning

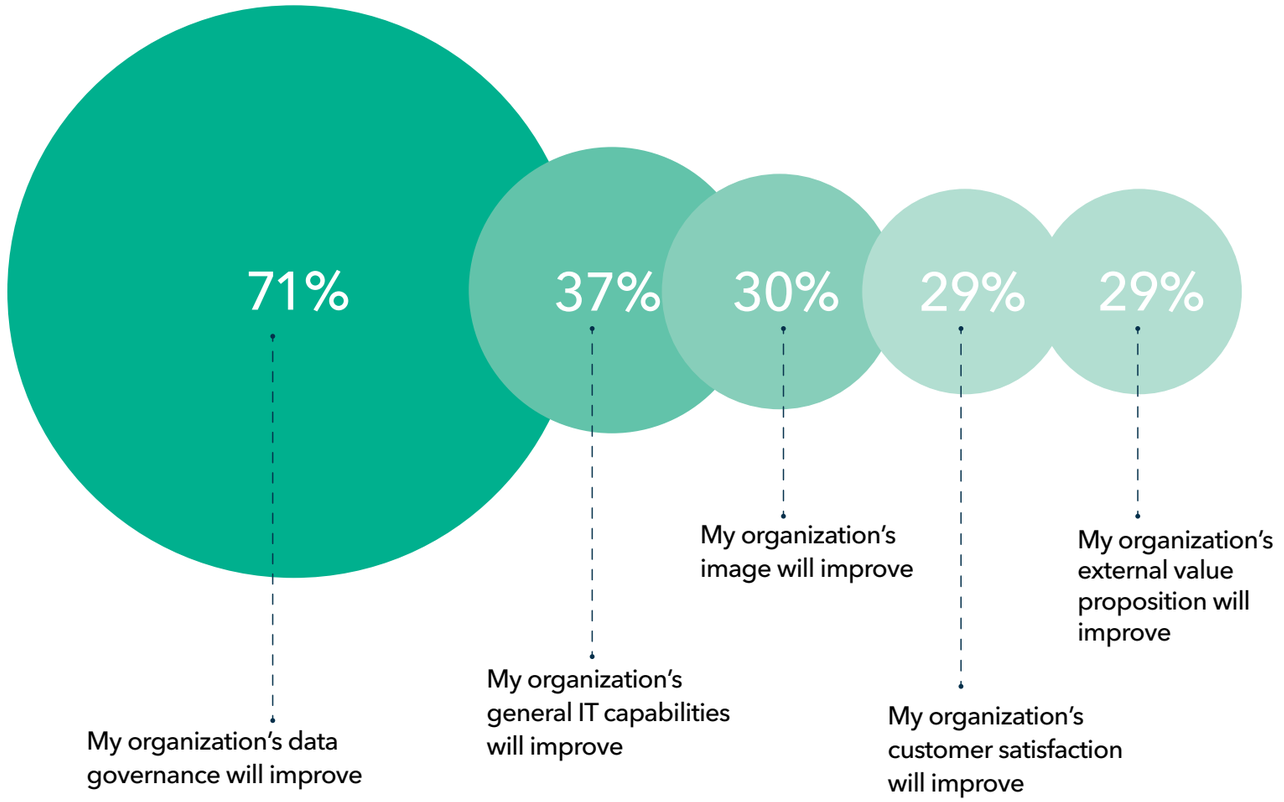
While the new GDPR rules are tighter and more challenging, the basic principles are the same as those we've had for many years. In that sense, for many companies the GDPR will be more about reviewing compliance procedures than building something from scratch. Whatever that entails for your company, the GDPR brings with it many benefits that can help your organization thrive.

1

## Improve data governance to drive business efficiency

The survey confirmed the opportunity of business benefits raised by the GDPR – 71 percent said the biggest opportunity is that working toward GDPR compliance can improve data governance. In turn, better data governance will contribute to the organization's efficiency. The survey showed that 37 percent of organizations think that their general IT capabilities will improve as they seek to comply. And 30 percent are convinced that complying with the GDPR will improve their image.

**Question:** What opportunities do you anticipate from your organization becoming GDPR compliant?

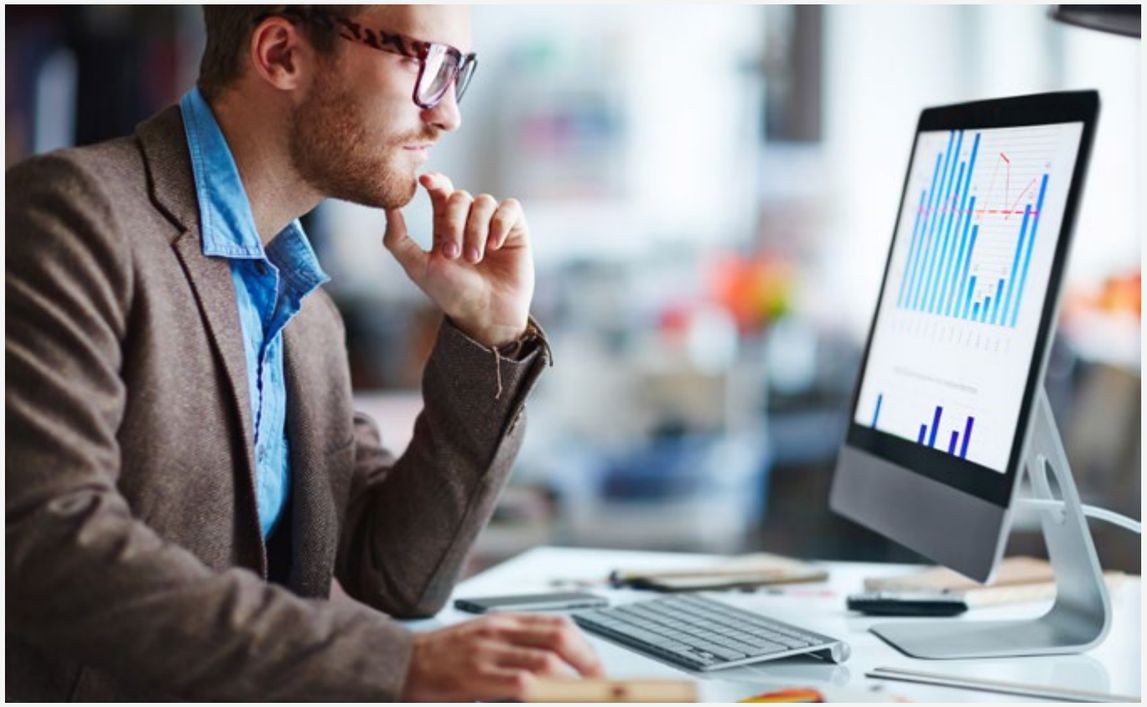


# 2

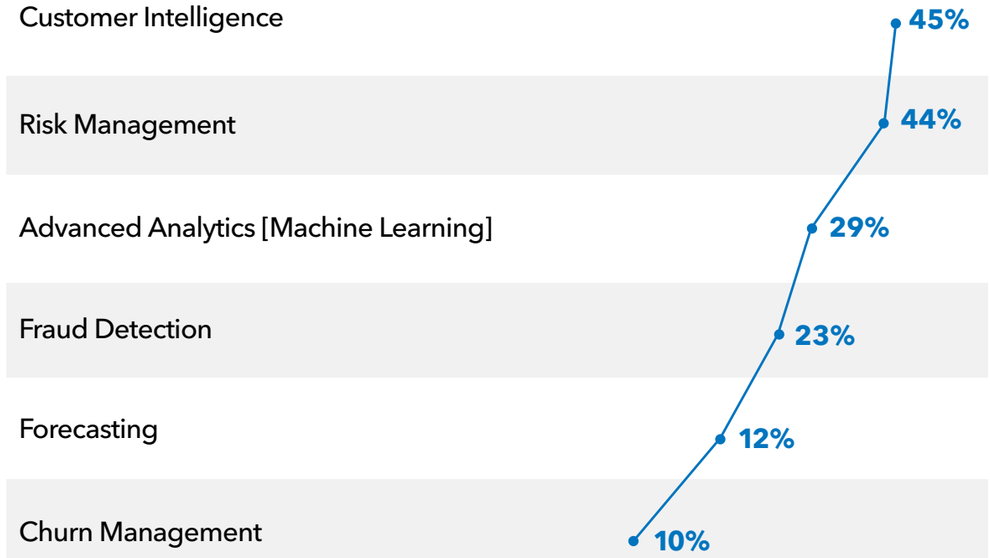
## Gain a competitive advantage

The GDPR gives organizations the opportunity to reassess all the data governance policies they're currently using. Not only for personal data, but for all data. Data – in constantly growing amounts – is one of the most important assets any business can have. With the correct policies in place, companies can not only comply, but also build a competitive advantage. Think about the possibilities of improving analytical processes, optimizing operational efficiency and reducing costs.

Respondents are aware of these benefits, acknowledging that the departments responsible for customer intelligence and risk management will profit the most from GDPR compliance. Financial and communications organizations in particular think the GDPR will be beneficial to departments working with advanced analytics. This is no surprise since personal data is at the center of many analytics initiatives.



**Question:**
GDPR could be considered as a catalyst for digitalization. Based on this premise, which one of your analytical business initiatives should benefit the most from GDPR?




Which business initiatives will benefit most from the GDPR?

3

## Achieve higher customer satisfaction

The GDPR benefits not just organizations – customers can also reap the rewards of compliance efforts. The survey shows that 29 percent of organizations think their customer satisfaction will be higher as they work toward GDPR compliance. Another 29 percent say their organizations' external value propositions will improve. New services and initiatives aimed at satisfying customers – such as individual data vaults – will also emerge as a result of companies needing to handle personal data with extreme caution.

With a holistic view of customer data – and insight into whether and how a customer wants to receive messages and actions – organizations can improve the customer experience by engaging in more relevant interactions. Government agencies, for example, could optimize their processes and improve citizen satisfaction by centralizing and securing shared personal information. That's true whether citizens interact in person at the town hall or through an agency's website.


### INTERAMERICAN expands personal data protection with SAS

"Our organization is working to transition to the new digital age and create long-term, trust-based relationships with our customers. To meet the new General Data Protection Regulation challenge in a timely way, we've chosen SAS to provide an integrated, end-to-end solution. SAS for Personal Data Protection will help us work toward compliance with the requirements of the new regulation and foster customer trust."

Xenophon Liapakis, CIO of INTERAMERICAN

Read more >

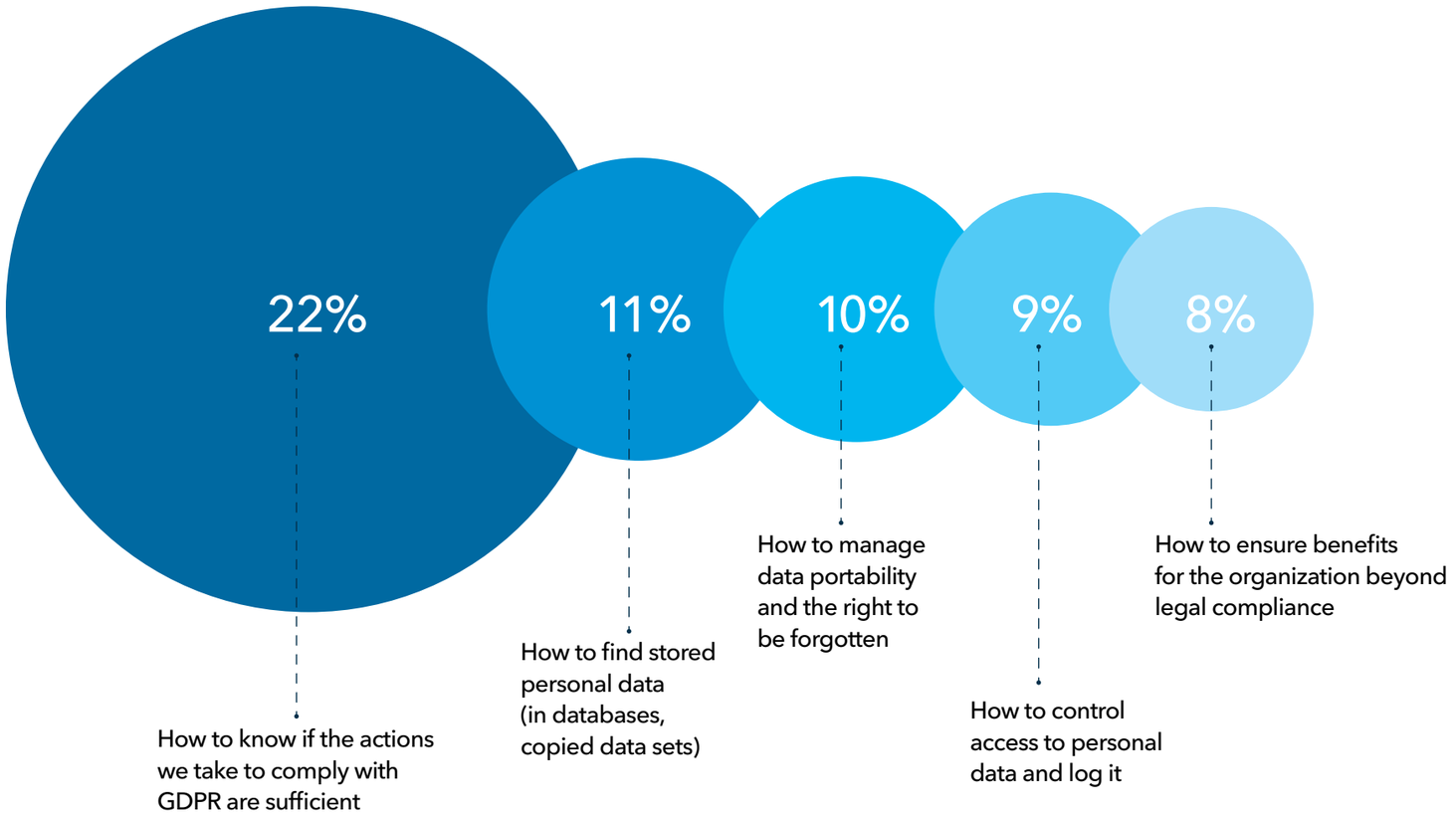
# Challenges of GDPR compliance

How do you know if the actions you've taken are sufficient?

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. But putting this into practice will require overcoming some hurdles.

The research results show that all organizations (98 percent) experience challenges in complying with GDPR. This is a bigger issue for respondents working in the EU government and health care sectors and in IT and services. Since the regulations are written in a general way, the biggest issue is knowing when the actions you've taken to comply are sufficient. Organizations are looking for clearer guidelines about this. Organizations in non-EU countries need this guidance even more, because they have generally been less exposed to data protection regulations than companies in the EU.

**Question:** What is your biggest challenge in preparing for the GDPR?



## Portability and the right to be forgotten

Of the surveyed organizations, 58 percent have problems managing data portability and the so-called right to be forgotten. Controlling access to personal data is also a serious challenge, especially for medium-size organizations of 51 to 500 employees. Large organizations and financial institutions have more difficulty finding stored personal data than other organizations. One reason is that this is a new, complex requirement – and it's the first time organizations have needed to consolidate and map full data from individuals for regulatory purposes.

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. Almost half of the surveyed organizations said that it was a challenge to find personal data within their own databases (copied data sets, CRM data, etc.).

While most companies are struggling with the tools and processes, many are also finding it hard to interpret GDPR guidelines on data portability. Take, for example, a telecom provider who has to be able to migrate all personal information, including contact details and photos, to another telecom provider when a consumer demands it. The original provider is obliged to deliver the data in a portable form. Accommodating data portability will be an enormous challenge for many telecom providers. The same goes for many other organizations, including utilities, retailers, banks and insurance companies.

**Question:**
Which of the following challenges do you see in preparing for GDPR?

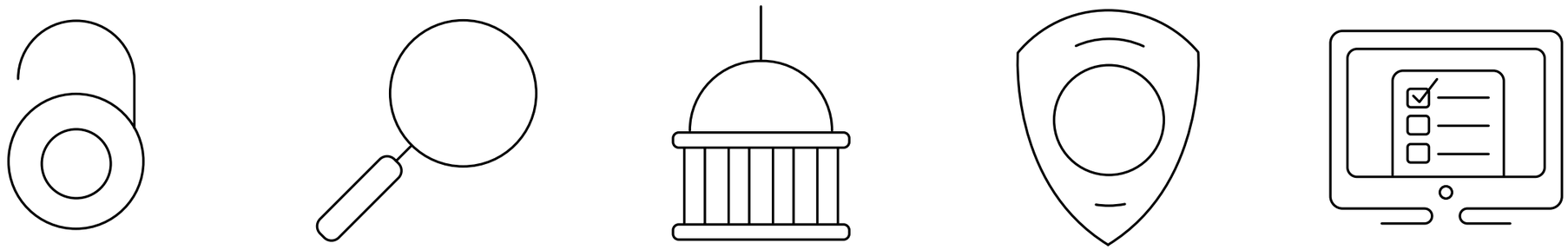
| | Total | EU | Non-EU |
|---|---|---|---|
| Knowing the actions we take to comply are sufficient | **59%** | 54% | 71% |
| Managing data portability and right to be forgotten | **58%** | 59% | 64% |
| Controlling access to personal data | **50%** | 52% | 45% |
| Finding stored personal data | **48%** | 48% | 50% |
| Complying with new profiling requirements | **44%** | 45% | 38% |
| Executing accurate Privacy Impact Assessments | **44%** | 43% | 45% |
| Dealing with consent management | **39%** | 38% | 40% |
| Ensuring benefits beyond legal compliance | **39%** | 38% | 45% |
| Accurate record keeping | **38%** | 38% | 38% |
| Management of poor personal data quality | **36%** | 36% | 38% |
| Adequate response to personal data breaches | **36%** | 35% | 36% |
| Forming a project team for compliance | **28%** | 28% | 21% |
| Knowing whether to appoint a data protection officer | **24%** | 25% | 10% |
| *Average number of challenges* | **5.5** | 5.4 | 5.5 |

# 5 steps to managing GDPR

Take an integrated approach

It's clear that noncompliance with the GDPR could be a real threat to the future of many organizations. But 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-Step Approach to GDPR



Access | Identify | Govern | Protect | Audit

1

**Access >** 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.

2

**Identify >** 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. Having the right tools in place for the job will make a big difference in your ability to meet the May 2018 GDPR deadline.

3

**Govern >** 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.

4

**Protect >** 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.

5

**Audit >** 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. While it may sound overwhelming, our five-step approach can make the path to GDPR compliance more manageable.

## 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 five-step approach is designed to guide you through these efforts, from gaining access to data sources to auditing the results. What's more, our 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 research 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.

## The main objective of this study involved:

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 and Insites Consulting. Recruitment via newsletters and several social media channels.

*How many employees work for your company worldwide?*

| **Survey stats:** Number of employees | **(NR) 347** Total | (NR) 103 Financial services | (NR) 41** Telco, media & communication | (NR) 62 Government & health care | (NR) 44** Chemical & manufacturing | (NR) 71 IT & services |
|---|---|---|---|---|---|---|
| Fewer than 50 | 16% | 8% | 5% | 13% | 11% | 37%* |
| 51 to 249 | 9% | 9% | 7% | 5% | 11% | 11% |
| 250 to 500 | 6% | 7% | 5% | 8% | 5% | 4% |
| 501 to 999 | 12% | 11% | 15% | 13% | 14% | 13% |
| 1000 to 4999 | 18% | 17% | 15% | 27%* | 25%* | 10% |
| 5000 or more | 36% | 46%* | 49%* | 32% | 32% | 25% |
| I don't know | 2% | 3% | 5% | 2% | 2% | 0% |

***Number of respondents (NR)**: 347*

*** Base size <50* *** Sig. Different from at least one other group (95%)*

*What is your role in your organization?*

| Role in organizations | Total (NR) 347 | Financial services (NR) 103 | Telco, media & communication (NR) 41** | Government & health care (NR) 62 | Chemical & manufacturing (NR) 44** | IT & services (NR) 71 |
|---|---|---|---|---|---|---|
| Information Technology | **30%** | 28%* | 34%* | 37%* | 37%* | 14% |
| Business Consultant | **19%** | 20%* | 22% | 10% | 10% | 27%* |
| Executive / Director | **17%** | 15% | 12% | 23% | 23%* | 24%* |
| Marketing / Sales | **12%** | 14%* | 15% | 8% | 8% | 14%* |
| Legal / Compliance / Privacy | **10%** | 15% | 10% | 6% | 6% | 11% |
| Data Protection Officer | **4%** | 5% | 5% | 5% | 5% | 1% |
| Information Security | **3%** | 2% | 2% | 3% | 3% | 7% |
| Human Resources | **2%** | 1% | 0% | 3% | 3% | 0% |
| Other | **3%** | 1% | 0% | 5% | 5% | 1% |

***Number of respondents (NR)**: 347*

*** Base size <50* *** Sig. Different from at least one other group (95%)*

*In which industry is your organization mainly operating?*

| Industry | (NR) 347<br>Total |
|---|---|
| Financial services | 30% |
| Telco, media & communication | 12% |
| Government & health care | 18% |
| Chemical & manufacturing | 13% |
| IT & services | 20% |
| Other | 7% |

***Number of respondents (NR)***: *347* *** Base size <50* * Sig. Different from at least one other group (95%)*

*What challenges do you see in preparing for GDPR?*

| Challenges | (NR) 347 Total | (NR) 239 EU | (NR) 42** Non-EU |
|---|---|---|---|
| Knowing the actions we take to comply are sufficient. | **59%** | 54% | 71%* |
| Managing data portability & right to be forgotten | **58%** | 59% | 64% |
| Controlling access to personal data | **50%** | 52% | 45% |
| Finding stored personal data | **48%** | 48% | 50% |
| Complying with new profiling requirements | **44%** | 45% | 38% |
| Executing accurate Privacy Impact Assessments | **44%** | 43% | 45% |
| Dealing with consent management | **39%** | 38% | 40% |
| Ensuring benefits beyond legal compliance | **39%** | 38% | 45% |
| Accurate record keeping | **38%** | 38% | 38% |
| Management of poor personal data quality | **36%** | 36% | 38% |
| Design adequate response to personal data breaches | **36%** | 35% | 36% |
| Forming a project team for compliance | **28%** | 28% | 21% |
| Whether to appoint a DPO | **24%** | 25%* | 10% |
| *Average number of challenges* | **5.5** | 5.4 | 5.5 |

**71%**

of non-EU organizations wonder if the actions they've taken to comply will be sufficient.

***Number of respondents (NR)**: 347*

*** Base size <50* *** Sig. Different from at least one other group (95%)*

*To what extent do you agree with these statements?*

| Do you agree with the statements below? | **(NR) 347** Total | (NR) 103 Financial services | (NR) 41** Telco, media & communication | (NR) 62 Government & health care | (NR) 44** Chemical & manufacturing | (NR) 71 IT & services |
|---|---|---|---|---|---|---|
| GDPR will have large effects on the IT of my organization | **67%** | 72% | 76% | 61% | 64% | 65% |
| My organization is aware of GDPR | **65%** | 72%* | 59% | 56% | 68% | 59% |
| GDPR will help to implement real data governance across my organization | **61%** | 63% | 61% | 69%* | 52% | 52% |
| My organization is already taking the necessary steps to prepare for GDPR | **56%** | 65%* | 51% | 48% | 50% | 56% |
| GDPR will have large effects on the business of my organization | **55%** | 49% | 66% | 61% | 52% | 56% |
| I am well informed about GDPR | **54%** | 53% | 56% | 60% | 48% | 54% |
| GDPR will positively affect the trust between my organization and its customers | **53%** | 47%* | 59%* | 55% | 50% | 58% |
| My organization is fully aware of the impact GDPR will have on the organization | **42%** | 47% | 56% | 26% | 43% | 42%* |

***Number of respondents (NR)***: *347*

% top 2 answers on a 5-point agreement scale

*** Base size <50*

** Sig. Different from at least one other group (95%)*

*GDPR could be considered as a catalyst for digitalization. Based on this premise, which one of your analytical business initiatives should benefit the most from GDPR?*

| Initiatives that will benefit most from the GDPR | **(NR)347** Total | (NR)103 Financial services | (NR)41** Telco, media & communication | (NR)62 Government & health care | (NR)44** Chemical & manufacturing | (NR)71 IT & services |
|---|---|---|---|---|---|---|
| Customer Intelligence | **45%** | 49% | 46% | 37% | 41% | 46% |
| Risk Management | **44%** | 41% | 32% | 45% | 48% | 46% |
| Advance Analytics [Machine Learning] | **29%** | 38%* | 39%* | 27% | 27% | 21% |
| Fraud Detection | **23%** | 27% | 27% | 23% | 16% | 18% |
| Forecasting | **12%** | 13% | 7% | 21%* | 7% | 8% |
| Churn Management | **10%** | 10% | 17% | 6% | 7% | 13% |
| None of the above | **16%** | 15% | 22% | 16% | 16% | 17% |

***Number of respondents (NR)***: *347*

*** Base size <50* *** Sig. Different from at least one other group (95%)*

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

**Follow us:**

To contact your local SAS office, please visit: sas.com/offices