CGOC
THE COUNCIL

RESOURCE GUIDE

GDPR READINESS STARTS WITH UNIFIED GOVERNANCE

CGOC
THE COUNCIL

Table of Contents

Why are so many organizations not ready?

In late 2017, the CGOC launched a survey of 132 corporate governance practitioners from around the world and across multiple industries to determine the level of GDPR readiness in their organizations.

For more than two years industry leaders, vendors and governments have warned organizations that GDPR could impact them and that compliance was not a simple proposition. Despite this, we had anecdotal evidence that many companies were not launching GDPR-readiness programs.

The Top Corporate Data Protection Challenges survey was an opportunity to gather some hard data. Even given our suspicions, the survey results surprised us. The gap between what organizations know they need to do and what they are actually doing is staggering.

In the following pages, we examine who the survey participants are and what their responses tell us about the state of data security and privacy regulation compliance.

The headline? Most businesses are not ready.

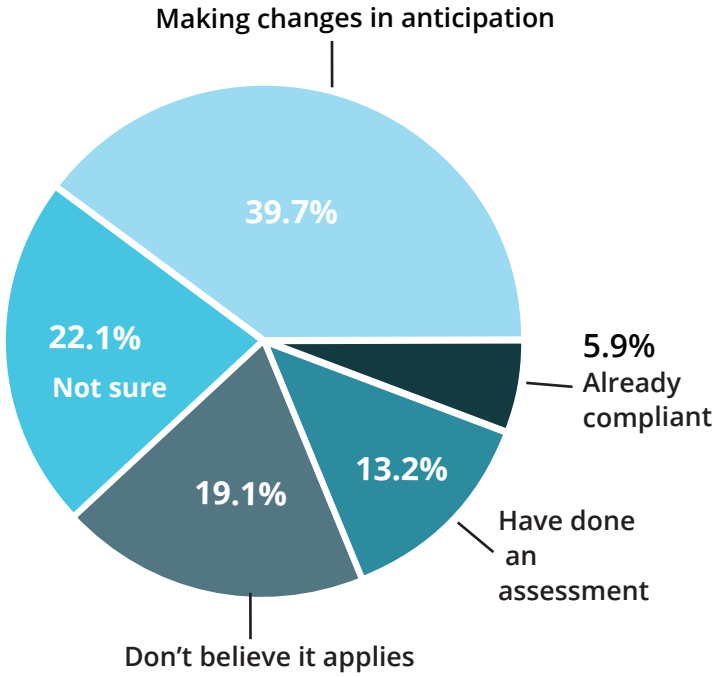
CGOC
THE COUNCIL

Implications: Organizational and Responsibility Gaps

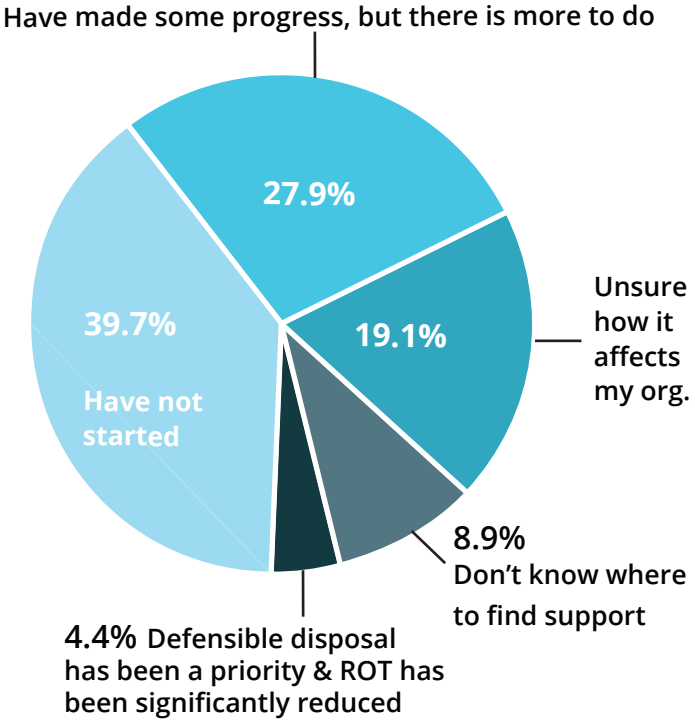
According to the Top Corporate Data Protection Challenges survey, only 6 percent of respondents felt their organizations were ready to comply with the GDPR — and these organizations face many other data protection and management challenges as well.

While this rather shocking lack of preparation can be explained in part by another survey response — that many executives allow day-to-day operations to take precedence over compliance — the challenges to data protection are both broader and deeper.

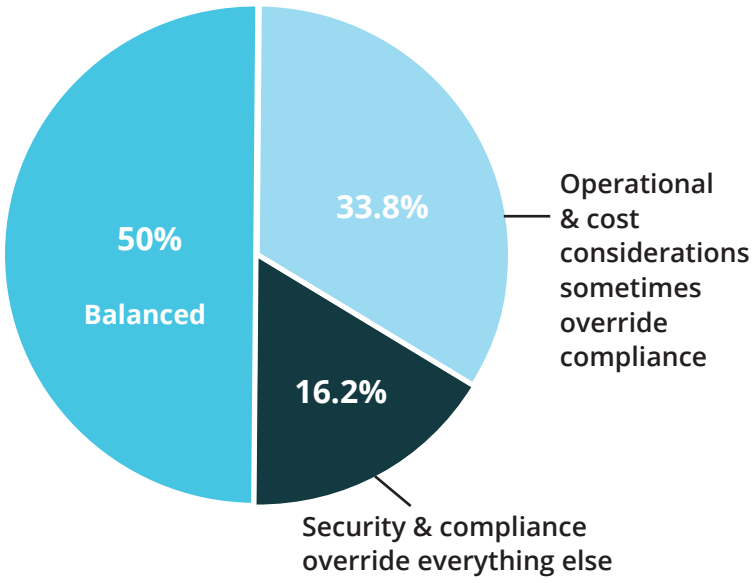
What is the status of your effort to comply with the upcoming EU General Data Protection Regulation (GDPR) in your organization?



Where is your organization in the process of defensible disposal of Redundant Obsolete and Trivial (ROT) data?



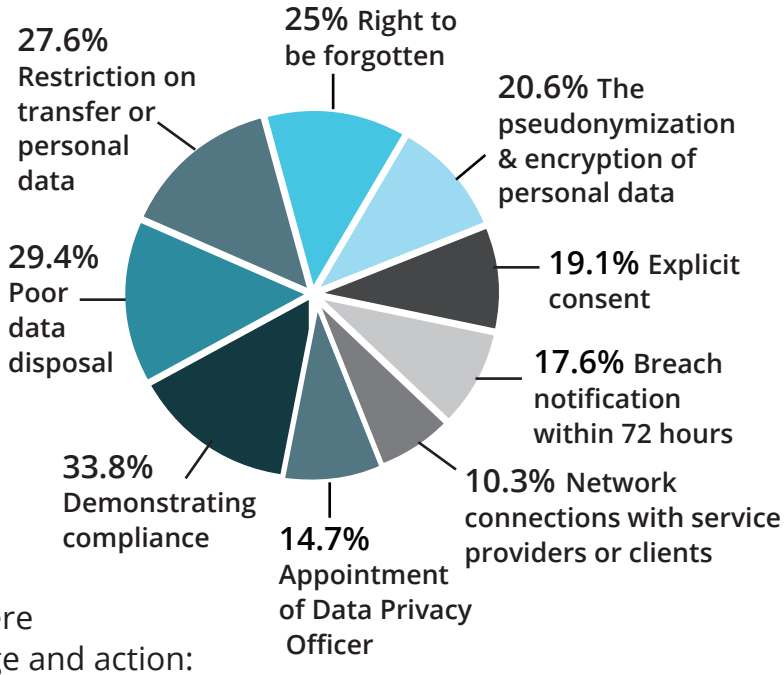
How would you describe the data protection risk/compliance appetite of your executives?



The two biggest roadblocks to GDPR compliance were believed to be poor data disposal practices and being unable to demonstrate compliance (i.e., survive an audit). Best practices around data disposal practices have been an area of concern for organizations for over a decade. This response indicates that despite the awareness and concern, confidence in enterprise data disposal practices remains low.

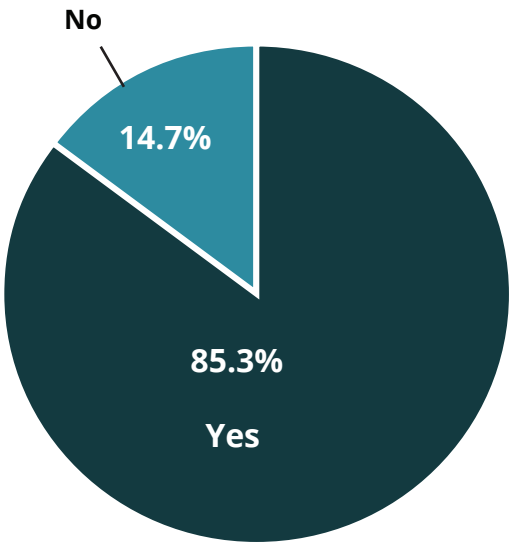
Similarly, while 85 percent say fine-tuning a defensible disposal program would benefit their data protection initiatives, 40 percent have not even started one.

Which GDPR requirement will create the most issues for your organization?

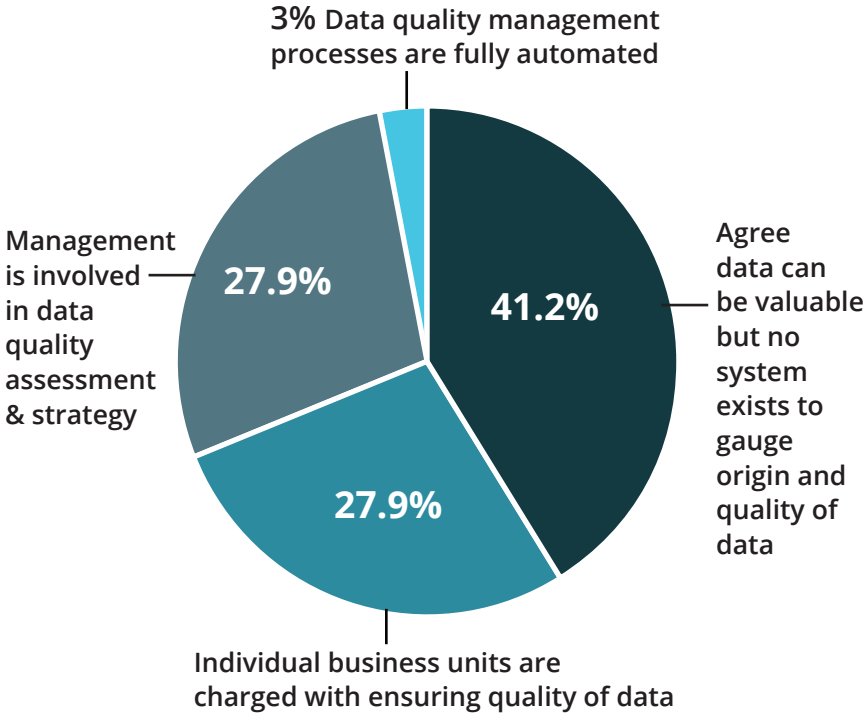


The survey sheds light on another area where there is a significant gap between knowledge and action: data lineage. Although most respondents understand the value of data to their organizations, 41 percent have no system in place to determine the origin and quality of that data, and only 3 percent have fully automated processes related to data quality and lineage with audit trails to ensure accuracy.

Where is your organization with regard to understanding data quality and lineage?

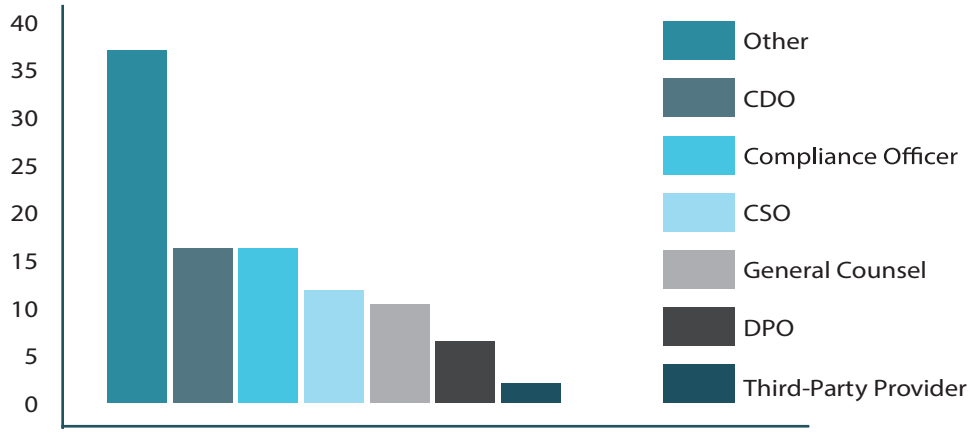


Do you believe fine-tuning your organization's defensible disposal program will assist in current and future data protection initiatives?



Inconsistent management is also a challenge. According to the survey, responsibility for GDPR compliance is spread among several different organizational roles. Particularly troubling is that nearly 37 percent of respondents chose "Other." Who are these individuals and what is their background? This inconsistency leads to different frames of reference regarding the importance of the compliance mission, the risks associated with data privacy and compliance failures, the prioritizing of readiness tasks and projects, and the ability to achieve results.

Who is the executive sponsor responsible for GDPR compliance in your organization?

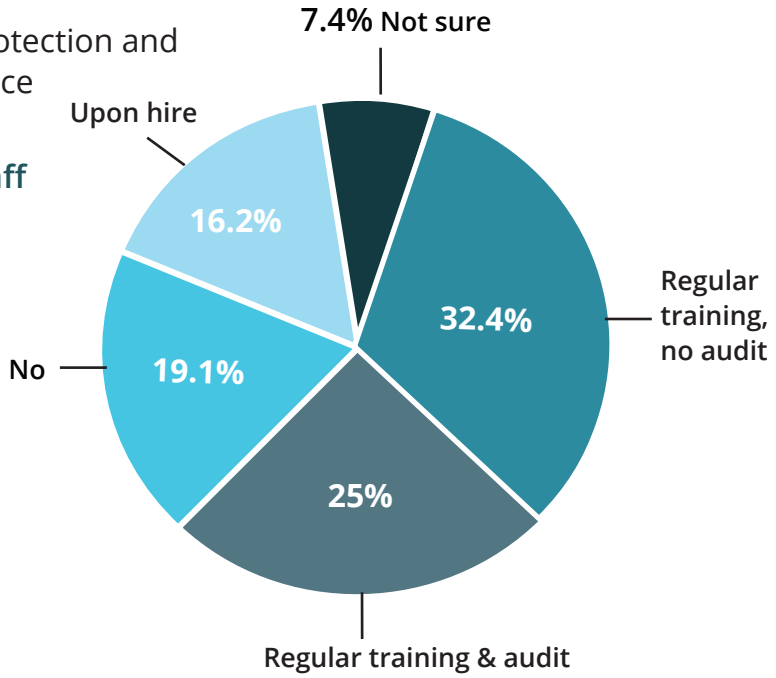


The Uber breach is a good example of what can happen when the privacy responsibility is poorly distributed and not in the hands of a fully independent Chief Privacy Officer. Inconsistency can also explain the wide variety of responses to questions about which GDPR requirements will create the most issues for the organizations and where organizations are most vulnerable to data theft, loss or exposure.

A final revealing area of the survey is training. Despite the increasing awareness of the threats to data and the potential for financial and reputational damage to organizations, only 57 percent of responding organizations train staff on data protection compliance, and only 25 percent conduct regular training with audits. One-time training without reminders and audits will do little to reduce the risks of significant fines under GDPR.

It's clear that despite all the threats, data protection and regulatory compliance have limited resonance at the highest levels of many organizations.

Does your organization train and audit staff on data protection compliance using the data protection rules that apply in your organization?



Corporate Compliance Insights
THE PREMIER SOURCE OF NEWS FOR TODAY'S GRC PROFESSIONAL

December 2017

Stop Dragging Your Feet: GDPR Compliance Can Make You More Competitive

By Heidi Maher, Executive Director, CGOC

According to a recent global CGOC survey of compliance officers only 6 percent of respondents felt their organizations were ready to comply with the regulation. The survey also reveals that these organizations face many other data protection and management challenges. This article discusses the findings of the survey.

One possible explanation for the lack of progress – as suggested in the survey data – is that many executives are too focused on day-to-day operations to worry about preventing a potential compliance problem down the road. But whether the lack of progress is caused by a mandate to increase earnings, a focus on improving the customer experience, or some other time-sensitive initiative, executives must understand that GDPR compliance isn't just about risk reduction and cost avoidance. The very same capabilities, strategies and technologies that enable GDPR compliance will help companies meet all their other business goals, including becoming a more efficient, more competitive organization.

A GDPR-Readiness program with a Unified Governance foundation can increase productivity while reducing costs and risk.

And it all starts with a Unified Governance program that provides a single, centralized view of all information across the enterprise and that automates critical information management processes.

MOST ORGANIZATIONS ARE MISSING THE BOAT

The GDPR harmonizes the various data protection laws in the EU that arose following the adoption of the European Data Protection Directive in 1995, which created only minimum standards around protecting the personal information of citizens and residents. Unlike the Directive, the new regulation also applies to all companies processing personal data of anyone residing in the EU, regardless of the company's location.

This means companies around the world must comply if they want to do business in the EU. Additionally, the consistency of the GDPR across the EU will likely lead to more consistent enforcement and penalties.

To successfully comply with the GDPR, organizations must know the type, value and location of the information they store, and they must be able to delete, change or provide information as required by the regulation. Yet Top Data Protection Challenges, a survey conducted by the CGOC, indicates that most organizations are not ready. The survey of 132 compliance officers from organizations around the world and across multiple industries revealed the following:

- Only 6 percent of respondents feel their organizations are compliant with GDPR requirements. Most organizations are also concerned about an inability to demonstrate compliance and revealing their poor data disposal practices.
- More than a third of executives, 34

percent, will sometimes let operational and cost concerns override compliance with data protection regulations.
- Only 57 percent of organizations train staff on data protection compliance, with only 25 percent doing regular training and
- Despite all the data breach headlines, 50 percent of respondents identify internal staff and practices as the biggest security threat vs. just 38 percent who choose external hackers. Notably poorly classified content is the third highest concern.
- One of the biggest surprises is that although 85 percent of respondents say fine-tuning a defensible disposal program will benefit data protection initiatives, 40 percent have not even started one.

GDPR, UNIFIED GOVERNANCE, & INCREASED COMPETITIVENESS

Why are organizations so ill-prepared when it comes to GDPR-readiness and other data protection and management challenges? Most likely because the frame of reference for these challenges is around the "potential" for breaches and fines. And it's difficult to deal with potentials when the realities of increasing revenue and improving customer service are so pressing.

But by solving the GDPR-readiness challenge, by arriving at a full understanding of the value and location of information and improving the ability to manage data deletion, organizations can provide new opportunities for every other information stakeholder:

- Executives can make better decisions based on the analysis of only the most relevant, high-quality information.
- Sales, marketing and customer service teams can increase their effectiveness and strategies by accessing consistent, up-to-date customer information.
- Product design and production teams can increase efficiency and accuracy by accessing reliable, up-to-date supplier and logistics data.
- Security teams can more quickly and easily identify the high-value and sensitive information they actually need to protect.
- Legal teams can more efficiently respond to retention requests while eliminating the risk of turning over more information than necessary during e-discovery.

Once businesses recognize the tremendous value across the enterprise of GDPR-readiness, the obvious question is how to get there. The answer is a comprehensive, Unified Governance program.

The key principles of a Unified Governance program include:

- Participation by representatives from all information stakeholders, including Legal, Records, Compliance, Security, HR, lines of business and IT, along with strong executive management support to ensure universal participation and long-term funding.
- Comprehensive and inclusive information policy management across the entire enterprise using a Master Datamap.
- Elimination of information silos to increase accessibility and facilitate management through a single automated and auditable process.
- Differentiation of high-value actively used data from redundant, outdated or trivial data.

The last bullet, which cannot occur without accomplishing the first three, is particularly important to GDPR readiness and increasing competitiveness. Only through this differentiation can the compliance team and business users gain ready access to high-value data without spending time sifting through "data debris."

Differentiation also enables the creation and maturing of a defensible data disposal program that automates the elimination of this debris, that is, all information with no legal, compliance or business value. The CGOC estimates that 69 percent or more of enterprise data is debris, so a defensible disposal program not only significantly reduces the burden on the GDPR compliance team, but also directly contributes to all the other hoped-for business benefits.

GDPR compliance is the headline, but a more competitive business that increases sales, reduces costs and minimizes risks is always the aim. By understanding that the underpinning of GDPR-readiness is a Unified Governance program that helps accomplish all these goals, organizations can more easily justify the required investment. For more information about how to launch and mature a Unified Governance program at your organization, visit www.cgoc.com.

***Heidi Maher** is an attorney and a legal technology specialist who has advised hundreds of organizations on information governance around data security, compliance and eDiscovery. She is the Executive Director of the CGOC, a forum of over 3,600 legal, IT, records and information management professionals from corporations and government agencies. For over a decade, CGOC has been advancing governance practices and driving thought leadership across the industry. Previously, she was a legal subject matter expert for a fortune 150 technology company, a felony prosecutor, a litigator and an assistant state attorney general. Heidi is a Certified Information Privacy Manager.*

Five Essential Steps to GDPR Survival

Written By: Eckhard Herych, CGOC Faculty Member

We are now less than a year away from the implementation of the European Commission's General Data Protection Regulation (GDPR) on May 25, 2018, and the stakes for companies are high. First, the GDPR "applies to all companies processing the personal data of data subjects residing in the Union, regardless of the company's location".

Second, non-compliant organizations can face devastating fines as high as four per cent of the annual global turnover or €20 million, whichever is higher. Third, preparing to meet the r equirements of the GDPR cannot be done overnight simply by deploying security software, which, unfortunately is where too many GDPR response discussions start.

The good news is that companies that begin now can make tremendous progress toward creating a data infrastructure that dramatically reduces the likelihood of GDPR non-compliance and that minimizes the financial impact even if something goes wrong. Here are the five key steps organizations must take to get ready.

Unify data management strategically

In the face of the GDPR, other evolving regulations, and advances in technology, data management and governance practices must be unified and auditable across all geographies and lines of business, and across on-premises, private cloud, public cloud, and hybrid infrastructures. The first step to achieving this is recognizing that every executive, manager and user has a stake in data management. C-level champions are essential, and CIOs, CDOs, and privacy officers must take the lead. This initiative must directly connect the data management, information security, legal and information governance teams, along with the lines of business.

Locate and understand the flow of all data

Stakeholders must work together to locate all data stores with collected information (such as customer data), created information {such as work product that might include customer data), and derived information (such as the results of analytics and machine learning that might include customer data).

They must understand the flow of information - the movement of data in business processes across multiple stakeholders (such as corporate counsel, strategic partners, etc.) and systems (such as legacy systems, cloud service providers, PCs, BYODs, etc.). Data mapping is an essential tool to create a visual depiction of how personal information flows across systems and devices as part of business processes. The map can include an overlay of GDPR requirements. In fact, the careful analysis of data flows in business processes is an essential component in our GDPR readiness assessment activities to ensure that our clients gain a sound understanding of their information landscape.

Evaluate all data

Only with the ongoing efforts of the first two steps can stakeholders evaluate the purpose or use of data and the regulatory obligations associated with it. Business users need to understand the value of the information they use to the organization. This is essential to helping all the key stakeholders (CIO, CDO, Privacy Officer, Legal, and InfoGov) assess:

What information is subject to GDPR?
- If data must be preserved, for how long? Is there a conflict between preservation requirements and GDPR requirements? If so, how will it be resolved?
- Is some data of "Legitimate Interest" to the organization for possible exemption from certain GDPR requirements (for example, GDPR Article 6 Lawfulness of processing)?
- Has consent been obtained for the intended use of the information (GDPR provides clear requirements and conditions to gain and establish consent)?

Dispose of all disposable data

Now that value has been assessed, it is possible to get rid of all data that has no business, legal or regulatory value, as well as all data that must be deleted to comply with the GDPR. In addition, now that IT knows where all the data is located, it is possible to ensure the proper deletion of all relevant data. This is critical to minimizing the impact of breaches and GDPR non-compliance. Moving forward, the deletion of obsolete data must become an integral part of operations to ensure that companies dispose of records or data in a controlled, legally defensible fashion.

Protect what's left

This is where most GDPR preparation discussions start, but only after following the first four steps is it actually possible to:

- Properly track the collection and movement of data
- Effectively control access to sensitive and private data
- Knowledgeably employ the most appropriate vendor security solutions, such as firewall, anti-virus, anti-phishing, etc.
- Automate disposal
- Provide employee training on data protection and privacy that has a chance of being effective
- Prepare for crisis management
- Establish processes and procedures to enable the organization to react to inquiries by authorities or individuals within the time frames defined in the GDPR

The inevitable GDPR time bomb is going off soon, and doing nothing to prepare for it beyond some new security measures and training is a recipe for costly data disasters. A real preparation effort will take time, and the sooner you start on this iterative journey, the better the position your organization will be in to avoid GDPR penalties or a least minimize their impact.

This article was first published on Infosecurity Magazine
www.infosecurity-magazine.com

CGOC
THE COUNCIL

Cross-Border Information Governance: Setting Yourself Up for Compliance

Speakers:

Dr. Andreas Splittgerber
Partner
Reed Smith LLP

Dorota Kosela
General Counsel
Braser S.A.

Cindy Compert
Data Security & Privacy
IBM Security

This CGOC-hosted, 60-minute on-demand webinar provides a detailed and thoughtful discussion among a panel of GDPR and privacy experts. The panelists discuss a range of international data protection regulations and mechanisms for international data transfers.

The webinar provides a great opportunity to hear firsthand:
- Risks that arise when controlling and processing personal data
- Myths associated with GDPR
- How to develop an effective Unified Governance plan to support cross-border GDPR compliance
- Tips for setting up internal systems to properly protect data

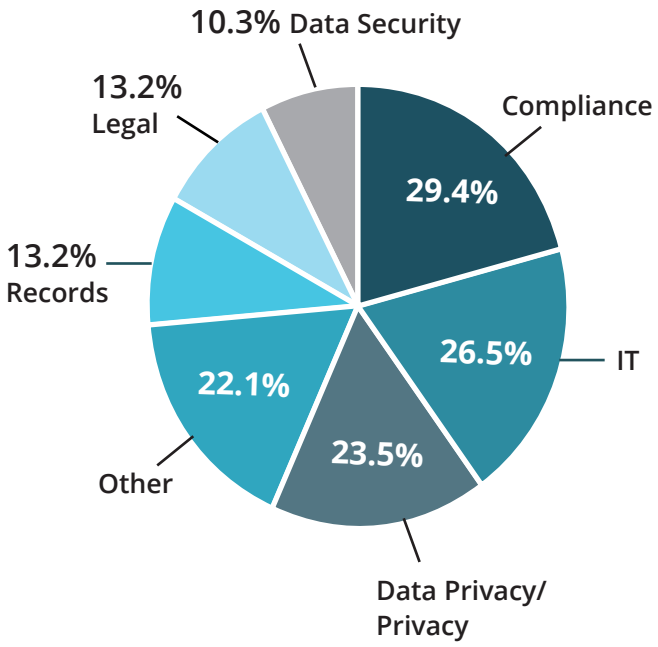
Watch the On-Demand Webinar on the
CGOC YouTube channel

CGOC
THE COUNCIL

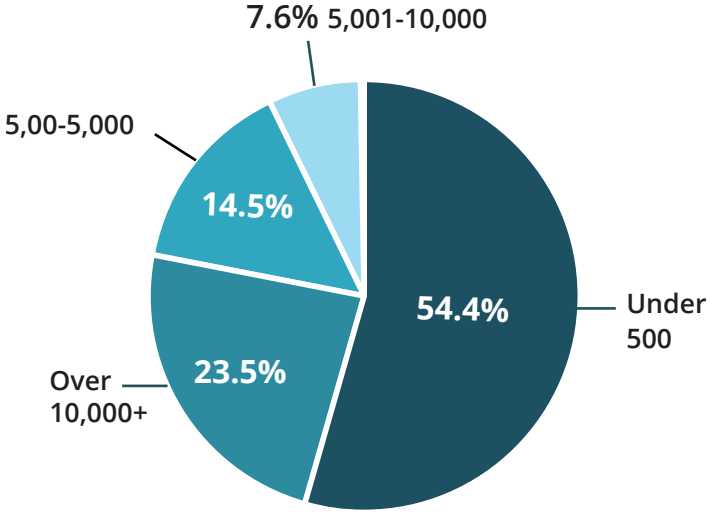
Appendix: Profile of Respondents

Our survey includes data from over 132 compliance officers from organizations around the world and across multiple industries.

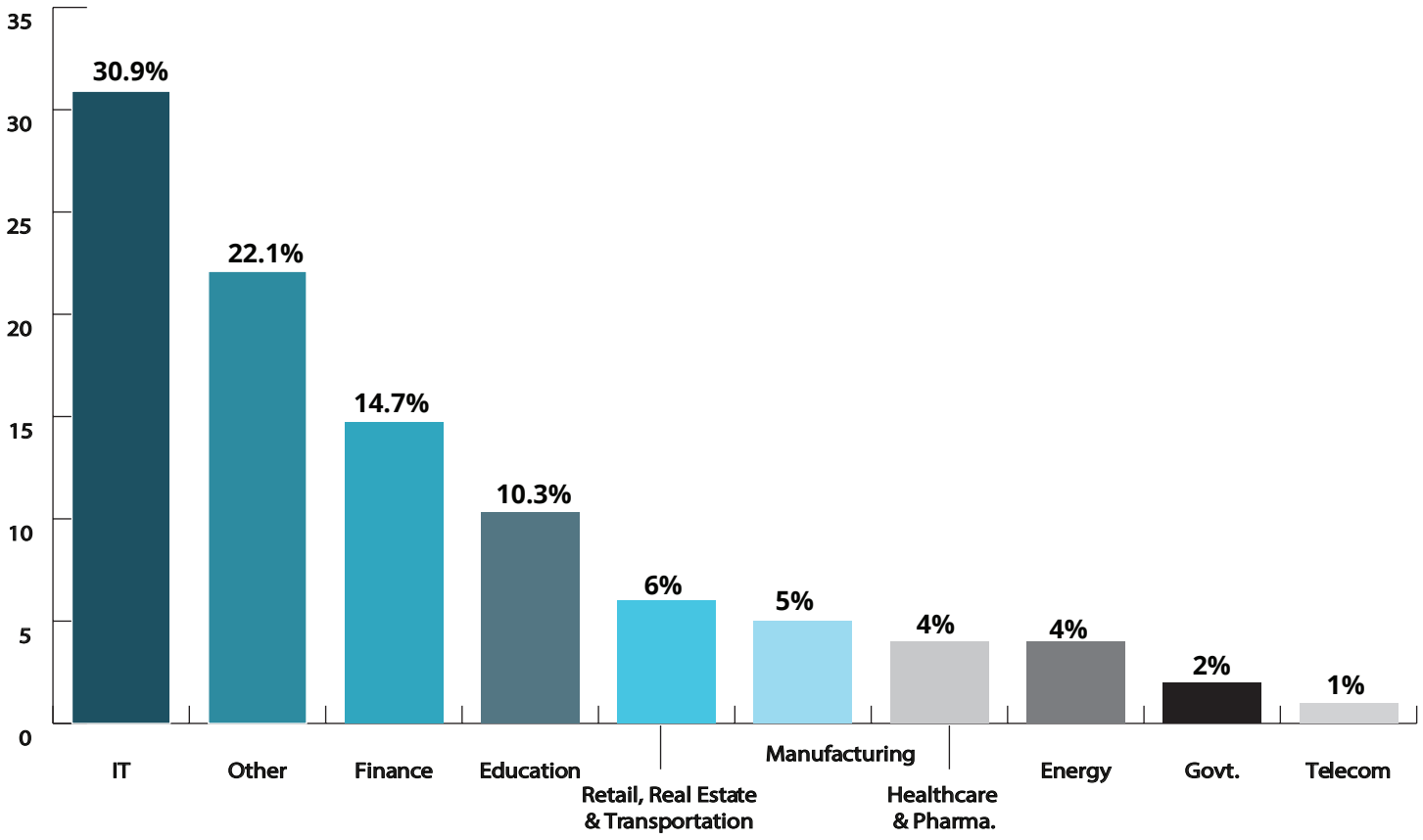
Respondent Job Function:



Organization size (employees):



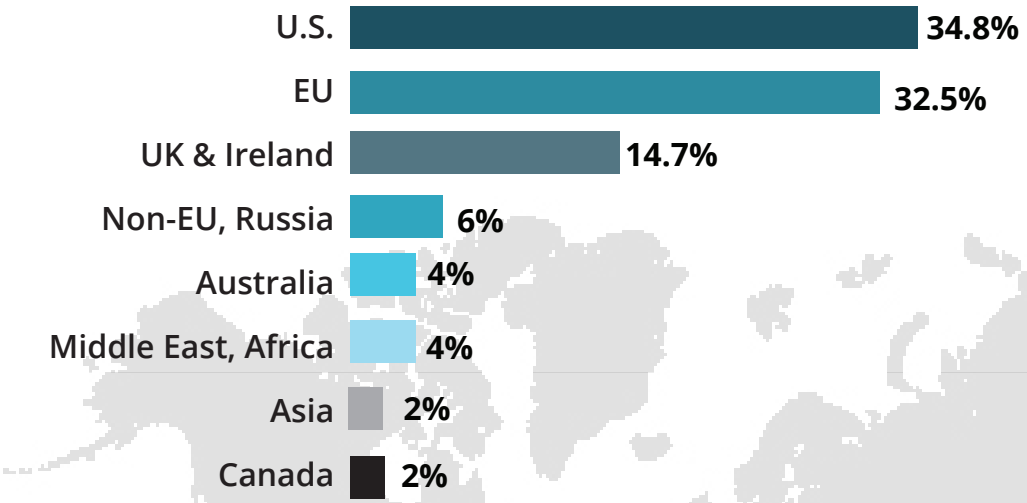
Industry:



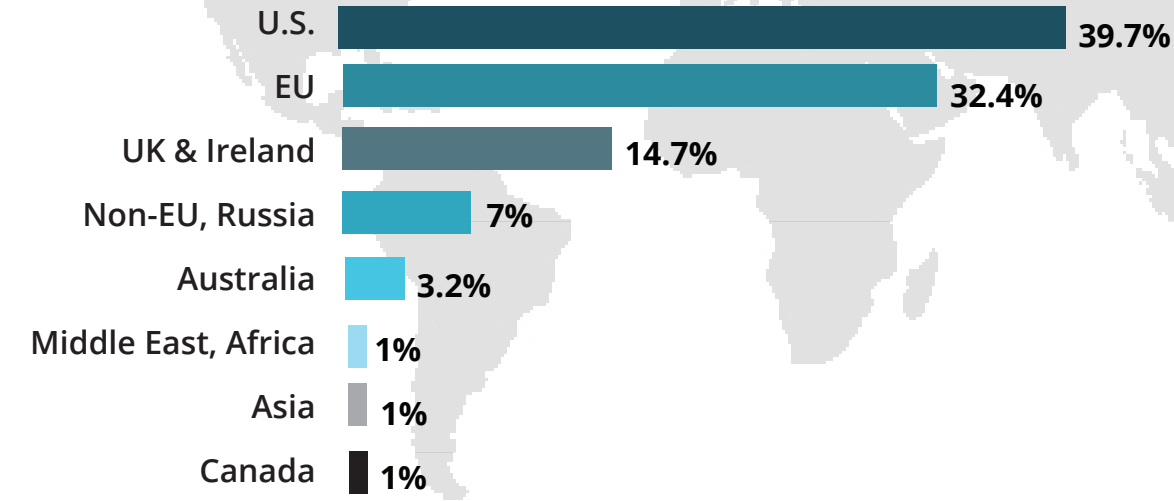
CGOC
THE COUNCIL

Appendix: Profile of Respondents cont.

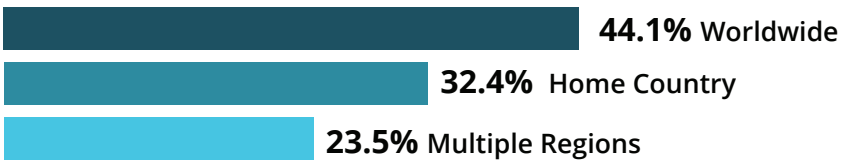
Region:



Headquarters:



Regions of Operation:



CGOC
THE COUNCIL

About CGOC

Through in-person events, executive meetings, webcasts, surveys and reports, CGOC helps executive leaders share ideas and advice with peers in an open and collaborative forum. Founded in 2004, CGOC fills the critical practitioners' gap between the EDRM and The Sedona Conference. Its charter is to create a forum that provides executives with the insight, interaction and information they need to make good business decisions. Join the CGOC Community!