

GDPR

THE END OF THE BEGINNING



ISACA[®]



EXECUTIVE SUMMARY

Just over six years ago, the European Union (EU) found itself at a unique moment in its technology history: the beginnings of the General Data Protection Regulation (GDPR). In January 2012, EU Justice Commissioner and former Vice President of the European Commission Viviane Reding memorably stated that “European data protection rules will become a trademark people recognize and trust worldwide.”¹ Those remarks touched off years of analysis, deliberation and decision-making that impacted nearly every aspect of the EU, at the personal, organizational, industrial and marketplace levels. It was an ambitious goal, one that saw the GDPR enter into force in 2016, with full enforcement in May 2018. Entities doing business in or with the EU must be in compliance by that date.

THE ENACTMENT OF GDPR IS NOT AN END, BUT A BEGINNING

However, the enactment of GDPR is not an end, but a beginning. Despite years of extensive discussion with an array of stakeholders, the reasons for the enactment of the GDPR are still evolving, and so is the global digital marketplace the GDPR will affect. While the EU, as a geographic region, has been a global leader in the implementation of data protection measures like the GDPR, other geographies are struggling to enact similar measures. Likewise, some industry sectors have readily embraced the requirements the GDPR has placed upon their constituent organizations, while others have not.

The story of GDPR, to this point, is only the prologue. Over the coming years, the real story will unfold, as industries and geographies incorporate it into their operations, their future plans and their legal, regulatory and public policy environments. We already have begun to see the initial GDPR effects. Israel, Argentina, Canada, Uruguay, New Zealand and the United States, as well as several other countries, have been deemed “third countries” by the EU², indicating that those nations’ data privacy protections are sufficient to enable personal data to flow unimpeded from EU member nations to those nations, without requiring additional safeguards. As the world becomes more used to doing business with the EU in a GDPR-enacted world, other nations will develop policy, regulatory and statutory measures similar to GDPR. These changes will not merely affect nations, however; they will impact industries as well.

Employee awareness and education are critical components of ongoing GDPR compliance. Awareness of—and commitment to—well-defined security, data management, and privacy policies and procedures clearly need to be an integral part of every organization’s culture, from the top down.



CHRIS K. DIMITRIADIS
Ph.D., CISM, CRISC,
CISA, chair of ISACA’s
GDPR Working Group

One of the most practical and cost-effective ways organizations can support GDPR and other compliance requirements is to help employees understand the business value of the information they deal with on a regular basis. That way, employees become more aware of their responsibilities when it comes to handling and protecting data within the flow of work, providing added value to the ways organizations earn and maintain the trust of customers and employees.



TIM UPTON
CEO at TITUS

1. V. Reding, “The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age,” excerpted from remarks given 22 January 2012 at the Digital, Life, Design Innovation Conference

2. https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_en

THE GEOGRAPHY OF GDPR

ISACA's 2018 GDPR Readiness Survey examined many facets of GDPR, including how GDPR was being received across geographies and industries in the final buildup to the 25 May enforcement deadline. Survey results included both the expected (17% of respondents from the EU indicated that their preparations for GDPR compliance began more than two years ago) and the unexpected (the EU came in second to Latin America; 24% of respondents from Latin America indicated that their preparations for GDPR compliance began at least two years ago).

Despite the efforts that nations and industries around the world already have undertaken to become GDPR-compliant, there are still more chapters in the GDPR story waiting to be written. Even within Europe, 33% of survey respondents indicated that complete GDPR compliance may not be reached by their organizations until late 2018, and 17% indicate compliance will not occur until 2019 or later. Similar stories can be found in the Middle East, where 44% of those surveyed said they believed their organizations would take until at least the closing months of 2018 or longer to become 100% GDPR-compliant, and Latin America, where 42% of responses indicated similar timelines for full compliance within their organizations.

GLOBALLY, 59 PERCENT OF RESPONDENTS STATED THAT THEIR BIGGEST CONCERN IN PREPARING FOR COMPLETE GDPR COMPLIANCE—NO MATTER WHERE THEY WERE ON A TIMELINE FOR IMPLEMENTATION—WAS DATA DISCOVERY AND MAPPING

Delays in becoming GDPR-compliant have roots in both external and internal factors. Globally, 59 percent of respondents stated that their biggest concern in preparing for complete GDPR

compliance—no matter where they were on a timeline for implementation—was data discovery and mapping.

Organizations need to identify the personal data they have from EU residents and take the appropriate steps to ensure it was collected lawfully and protected appropriately.

When external factors are examined, the story takes on yet another twist. When asked how likely it would be that countries within a particular geographic region would use GDPR as a model for crafting data privacy legislation or regulations within the next year, respondents from all but one region expressed the belief that it would be their region that would be most likely to do so. The sole exception was North America, where only 57% of respondents believed such a course of action was likely or very likely to occur. Africa (78%), Asia (64%) and Latin America (67%) all felt more strongly than North American respondents that their region would be the more likely to see legislation in the spirit of GDPR.

A similar picture emerges when respondents were asked to consider the use of GDPR as a model for the crafting of data privacy legislation or regulations on a 3-5-year time horizon. North American respondents again demonstrate that that they do not believe as strongly as their global counterparts that North America will be likely or very likely to use GDPR in that region's legislative, regulatory or public policy efforts. Respondents from Africa (82%), Latin America (71%), Asia (68%) and the Middle East (66%) all believe more strongly than respondents from North America (64%) that North America will use GDPR in the creation or amendment of data privacy public policy. This lowered opinion among North American respondents may be due to any number of factors, including perceptions about data privacy public policy progress within the United States.

THE DEMOGRAPHY OF GDPR

Several interesting insights into how the GDPR was viewed by industry were revealed in ISACA's 2018 GDPR Readiness Survey. One of the most interesting was that, when asked if executives within their organization had made GDPR compliance a business priority, it was the pharmaceutical (81%), and advertising/marketing/media (75%) sectors that indicated the strongest affirmative response, outpacing even the financial/banking (71%) and technology services/consulting (74%) sectors. Overall, across all industries, 69% of all executives responded that they had made GDPR compliance a business priority.

It would also appear that—across all industries—there was already some level of concern about personal data protection prior to enactment of the GDPR. According to research results, across all industries, an average of approximately 62% of respondents indicated that their organizations already had in place data protection policies that guided employees on how to secure personal data. Such policies were especially prevalent in the telecommunications and communications industries (72%); the healthcare and medical industries (71%); the financial, banking and insurance industries (70%); and the pharmaceutical industry (67%).

WHEN ASKED WHEN 100% COMPLIANCE WOULD OCCUR, RESPONDENTS INDICATED THAT THE PUBLIC SECTOR (GOVERNMENT OR MILITARY AT THE NATIONAL/STATE/LOCAL LEVELS) WAS THE LARGEST AREA OF CONCERN

It was the public sector, however, and not the private sector, that provided perhaps the most worrisome insights into GDPR compliance. When asked when 100% compliance would occur, respondents indicated that the public sector (government or military at the national/state/local levels) was the largest area of concern. The respondents believed that the public sector's efforts to obtain complete GDPR compliance would

predominantly occur far after the GDPR's enactment, with 43% of responses indicating that it would be at least the closing months of 2018—and likely much later than that—before the public sector reached 100% compliance.

This makes sense, though. Traditionally, the public sector's revenue streams have been limited in scope, encompassing primarily taxes, fees and regulated gaming endeavors. While private sector industries readily innovate and evolve, the public sector often finds itself limited by the need to create legislation, regulations or policies that will generate additional revenue or create new revenue streams—and the subsequent need to get elected and appointed public officials to agree to write, pass, and implement those changes.

For those industries that have begun to prepare for GDPR, a picture similar to the regional geographic picture emerges. Data discovery and mapping was the leading challenge for all industries except the aerospace industry, much in the way it was the leading challenge across all global regions. Aerospace industry respondents indicated two other areas in which their concerns were greater: prioritizing GDPR compliance among other business priorities, and organizational education and change programs.

Some organizations, though, are not required to become GDPR-compliant—and presently, they are largely disinclined to do so. More than three-fourths (77%) of survey of respondents from organizations that are not required by law to comply with the GDPR had no plans to do so in 2018. However, that means that 23% of respondents and their organizations believed that it was in their enterprise's best interests to comply with the GDPR, even though it is not required. These 23%, it is likely, will be better prepared as data protection measures continue their proliferation throughout the global public policy, legislative and regulatory communities.

Survey respondents from Europe already share the mindset of those who would comply without being required to do so. When posed the same question regarding compliance with the GDPR, 48% of European respondents indicated that their organization would become GDPR-compliant in 2018. Contrast that with Asia (19%) and North America (17%), where dramatically lower levels of respondents indicated their organizations would become GDPR-compliant regardless of requirements.

Though it is understandable that some organizations in Asia and North America might see such “opt-in” compliance as an unnecessary additional business cost, this may prove short-sighted and ill-advised in the long run. ISACA’s 2018 GDPR Readiness Survey indicated that 37% of organizations anticipated that the total expected costs incurred to become GDPR-compliant was US \$5 million or less, with 27% of

respondents citing costs of less than US \$1 million. There is additional cost in complying with GDPR when not required to, but the cost of being “left behind” as the rest of an organization’s industry or marketplace becomes predominantly GDPR-compliant could be far greater.

There is at least a groundswell of organizations firm in their belief that their GDPR readiness preparations will serve their business efforts well. When survey respondents were queried about which positive outcomes they anticipated for their organization because of their preparations for the GDPR, 60% of global respondents cited greater data security, while 49% said they believed it would improve their organizations’ business reputations. Forty-three percent indicated that their GDPR readiness preparations efforts would better marry data security best practices with their corporate culture.

CONCLUSION

Judging from the responses to ISACA’s 2018 GDPR Readiness Survey, it is clear more chapters in the GDPR story will be written. In several countries, the writing of those chapters is already underway. Early in 2018, Australia’s data breach notification legislation went into effect; additionally, Australia is currently ramping up efforts within the APAC region to support cross-border data privacy efforts. India is creating a new data protection framework, as well as legislation focused on data privacy, while Argentina is working on enhancements to and the strengthening of its existing data protection authority, using legislation patterned on the precepts outlined in the GDPR. Earlier in 2018, Mexico implemented legislation that extends GDPR-like protection to data held by the various data protection authorities throughout the multiple levels of that nation’s public sector. Singapore is making changes to its Personal Data Protection Act to incorporate many of the key precepts contained within the GDPR, including mandatory data breach notification.

Industries are noticing these shifts, as well, and offering less resistance to measures such as the GDPR. While some industries may not welcome additional data privacy regulatory requirements out of concerns for incurred extra costs or reconfigured workstreams, other industries are realizing that regulations such as the GDPR are increasingly becoming part of the global digital marketplace landscape—and that many of their customers, clients, or constituents welcome the protections obtained from the GDPR and similar initiatives.

When protecting data, we can’t think in terms of nations—or even specific industries—any more. The digital economy is global and borderless, and the commingling of industries (e.g., online retailers becoming offering financial and banking services, etc.) demonstrates that even the borders between industries are crumbling. This will not change—it will only increase.

Going forward, it would be of benefit to think in terms of ecosystems—global, interrelated ecosystems of commerce, of law enforcement, of communication, of interaction and of countless other facets of our modern civilization. If we approach data protection from the standpoint of ecosystems, our actions must focus on hardening that ecosystem, making it more robust, globally.

This means that it is very likely that data protection public policy measures will become the norm, globally—not the exception. As emerging technologies arise and their impacts are felt in data protection, those new concerns must be taken into consideration when shaping the next generation of data protection legislation and regulation. This also means that the stakeholder group that participates in crafting the “nextgen” version of the GDPR must be both broad and deep, encompassing as many aspects and levels of the public and private sectors, academia, and the NGO community as possible. These groups all have a stake in the success of hardening data protection measures to benefit our global digital ecosystem.

The time to prepare for a data-driven future is before it arrives—not after. Regrettably, though, in some ways, we’re currently in the latter situation—and we can already see the challenges that brings with it. ISACA’s 2018 GDPR Readiness Survey finds that,

among organizations that need to comply with GDPR, only 39% of staff have been educated on their responsibilities required to maintain GDPR compliance, and only 29% of organizations believe they will be fully GDPR-compliant by the deadline for compliance. It is not easy to alter entrenched business practices, or conform to new requirements, even if those requirements might be beneficial to the organization and its lines of business. GDPR provides an opportunity for organizations to engage employees and hold them accountable for the safeguarding and protection of the personal data they handle. The positive business outcomes are clear from the survey data – organizations have an opportunity in front of them to improve the reputation of their business, have stronger collaboration across business units, connect data security practices with corporate culture, and build greater customer loyalty and engagement as a result.

There is a need to focus on the public policy, regulatory and legislative tools that will build in privacy and security by design, and ensure that, on an ecosystem level, there is strong cyber and information security as well as technology and information governance. The GDPR and similar data privacy and protection policy measures have a role to play in that future. The future is going to be here before we realize it—it’s up to us to set the pace, not just try to keep pace.

SURVEY METHODOLOGY

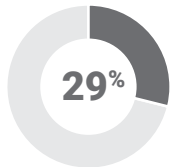
ISACA’s GDPR Readiness Survey reflects the perspectives of more than 6,000 business and technology professionals who are members of ISACA. The survey was conducted from 16-23 April 2018, with a margin of error of +/-1.3, at a 95 percent confidence level. Additional information is available at www.isaca.org/gdpr-readiness-survey.

ARE YOU READY FOR THE GDPR DEADLINE?

MOST ORGANIZATIONS ARE NOT.

The deadline for GDPR compliance is this month, but most enterprises say they are not prepared. Global technology association ISACA conducted a poll of more than 6,000 professionals worldwide who weighed in on their organizations' GDPR-readiness. See below to find out their top challenges with—and expected benefits from—compliance, and learn more at www.isaca.org/gdpr-readiness-survey.

THE BAD NEWS

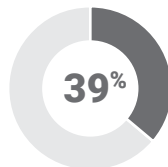


of organizations will be fully GDPR-compliant by the deadline.



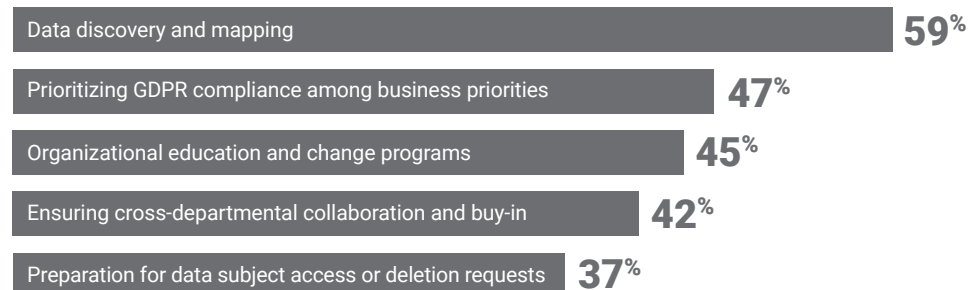
1 in 10

doesn't know whether his/her organization is required by law to be GDPR-compliant.

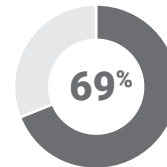


Staff have been educated on responsibilities to a satisfactory level to maintain GDPR compliance.

Top five challenges in preparing for GDPR compliance:

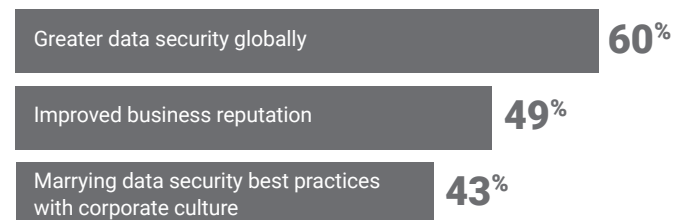


THE GOOD NEWS



Believe their executives have made becoming GDPR-compliant a priority.



The top three positive outcomes expected from their organization's GDPR preparation are:








ISACA'S GDPR READINESS SURVEY

Fielded 16 – 23 April 2018



Q1 TO THE BEST OF YOUR KNOWLEDGE, IS YOUR ORGANIZATION REQUIRED BY LAW TO BECOME GDPR COMPLIANT?

Answer Choices	Responses
Yes  65.00%	3591
No  35.00%	1934
	Answered 5525
	Skipped 0




Q2 HOW CONFIDENT ARE YOU THAT YOU KNOW WHETHER OR NOT YOUR ORGANIZATION IS REQUIRED BY LAW TO BECOME GDPR COMPLIANT?

Answer Choices	Responses
Extremely confident  35.84%	1980
Very confident  29.10%	1608
Somewhat confident  25.61%	1415
Not so confident  7.55%	417
Not at all confident  1.90%	105
	Answered 5525
	Skipped 0

Q3 IF YOUR ORGANIZATION IS NOT REQUIRED BY LAW TO BECOME GDPR COMPLIANT, DOES YOUR ORGANIZATION INTEND TO BECOME GDPR COMPLIANT IN 2018?

Answer Choices	Responses
Yes  23.22%	454
No  76.78%	1501
	Answered 1955
	Skipped 3570

Q6 DO YOU FEEL THAT EXECUTIVES WITHIN YOUR ORGANIZATION HAVE MADE BECOMING GDPR COMPLIANT A BUSINESS PRIORITY?

Answer Choices	Responses
Yes  68.98%	2633
No  16.11%	615
Don't know  14.91%	569
	Answered 3817
	Skipped 1708

Q8 WHEN DO YOU EXPECT YOUR ORGANIZATION WILL BE 100% GDPR COMPLIANT?

Answer Choices	Responses
By the 25 May 2018 deadline 28.66%	1094
Q3 2018 10.22%	390
Q4 2018 13.18%	503
Q1 2019 6.76%	258
Later than Q1 2019 10.14%	387
Don't know 31.05%	1185
	Answered 3817
	Skipped 1708

Q10 HOW SATISFIED ARE YOU WITH THE PROGRESS OF YOUR ORGANIZATION'S GDPR PREPARATION OVERALL?

Answer Choices	Responses
Very satisfied 10.95%	418
Satisfied 38.67%	1476
Neither satisfied nor dissatisfied 28.84%	1101
Dissatisfied 9.72%	371
Very dissatisfied 2.28%	87
Don't know 9.54%	364
	Answered 3817
	Skipped 1708






Q11 APPROXIMATELY WHEN DID YOUR ORGANIZATION BEGIN THE PROCESS TOWARDS GDPR COMPLIANCE?

Answer Choices	Responses
More than 2 years ago 14.36%	548
In the past 1 year 40.40%	1542
In the past 6 months 18.47%	705
In the past 30 days 3.43%	131
Not started 4.03%	154
Don't know 19.31%	737
	Answered 3817
	Skipped 1708

Q12 WHICH, IF ANY, OF THE FOLLOWING CHALLENGES/CONCERNS DOES YOUR ORGANIZATION HAVE IN PREPARING FOR GDPR COMPLIANCE? SELECT ALL THAT APPLY.

Answer Choices	Responses
Ensuring cross-departmental collaboration and buy-in	42.23% 1612
Organizational education and change programs	44.83% 1711
Data discovery and mapping	59.47% 2270
Preparation for data subject access or deletion requests	36.60% 1397
Preparation for breach notifications in 72 hours (under certain conditions)	27.59% 1053
Assessing what your organization needs to do to become compliant	34.87% 1331
Prioritizing GDPR compliance among other business priorities.....	46.92% 1791
Potential fines.....	20.04% 765
Possible business model interruption.....	15.04% 574
Cost of compliance.....	32.01% 1222
Integration with other data protection regimes in other regions/nations.....	24.97% 953
None of the above	6.37%.. 243
Other concerns (please specify)	3.64%.. 139
	Answered 3817
	Skipped 1708

Q13 APPROXIMATELY WHAT IS THE TOTAL EXPECTED COST TO YOUR ORGANIZATION TO BECOME GDPR COMPLIANT?

Answer Choices	Responses
Less than US\$1,000,000  26.57%	1014
US\$1,000,000 to \$5,000,000  38.67%	392
US\$5,000,000 to \$10,000,000  28.84%	127
Greater than US\$10,000,000  9.72%	122
Don't know  9.54%	2162
	Answered 3817
	Skipped 1708





Q14 WHAT, IF ANY, PROTECTIVE MEASURE (S) FOR PERSONAL DATA OR PII WERE IN PLACE AND ADHERED TO BY MOST EMPLOYEES PRIOR TO ANY GDPR IMPLEMENTATIONS IN YOUR ORGANIZATION? SELECT ALL THAT APPLY.

Answer Choices	Responses
Encryption of all (or majority of) PII stored either on-site or in the cloud.....	52.50% 1932
Robust data sharing and management policies.....	47.07% 1732
Technical controls restricting sharing and copying of data (on a USB, for example).....	58.53% 2154
Regular audits and deletion of old data, or data that was stored after initial use passed.....	39.92% 1469
Rigorous access controls over who can see certain types and categories of personal data.....	55.76% 2052
Post-data breach notification, recovery and response protocols in place.....	37.64% 1385
A data protection policy that guides employees on how to secure personal data	63.80% 2348
No specific PII relevant policies or practices	9.81% 361
Other protective measures (please specify)	2.31% 85
	Answered 3680
	Skipped 1845







Q15 WHAT, IF ANY, ARE THE ANTICIPATED POSITIVE OUTCOMES YOU EXPECT TO SEE FROM YOUR ORGANIZATION'S GDPR READINESS PREPARATION? SELECT ALL THAT APPLY.

Answer Choices	Responses
Improved business reputation.....	48.53% 1786
More engaged customers	21.79% 802
Competitive advantage in the EU	28.61% 1053
Improved business revenue.....	13.18% 485
Greater customer loyalty	27.53% 1013
More accurate data for analysis and insight.....	33.18% 1221
Required employee data protection training	37.61% 1384
Greater data security globally.....	59.67% 2196
Stronger collaboration across business units.....	26.17% 963
Marrying data security best practices with corporate culture	43.21% 1590
None of the above	7.17% 264
Other positive outcome anticipated (please specify)	2.50% 92
	Answered 3680
	Skipped 1845

Q16 APPROXIMATELY WHAT IS THE TOTAL EXPECTED COST TO YOUR ORGANIZATION TO BECOME GDPR COMPLIANT?

Answer Choices	Responses
Less than US\$1,000,000  27%	1015
US\$1,00,00 to \$5,000,000  10%	127
Greater than US\$10,000,000  3%	122
Don't know  57%	2162
	Answered 3818
	Skipped 1711

Q17 DO YOU THINK STAFF AT ALL LEVELS WITHIN YOUR ORGANIZATION HAVE BEEN EDUCATED TO A SATISFACTORY LEVEL ABOUT THEIR RESPONSIBILITIES TO MAINTAIN EVERYDAY GDPR COMPLIANCE?

Answer Choices	Responses
Strongly agree  6.90%	254
Agree  31.90%	1174
Neither agree nor disagree  25.79%	949
Disagree  21.98%	809
Strongly disagree  5.30%	195
Don't know  8.13%	299
	Answered 3818
	Skipped 1845

Q18 WILL YOUR ORGANIZATION PUT INTO PLACE CONTROLS TO MONITOR ONGOING GDPR COMPLIANCE?

Answer Choices	Responses
Yes 69.29%	2550
No 4.97%	183
Don't know 25.73%	947
	Answered 3680
	Skipped 1845

Q21 HOW LIKELY ARE THE FOLLOWING REGIONS TO USE GDPR AS A MODEL FOR CRAFTING DATA PRIVACY LEGISLATION OR REGULATIONS IN THE NEXT 12 MONTHS?

Very likely	Responses
Africa 2.83%	101
Asia 8.06%	289
Latin America 4.46%	158
Middle East 4.93%	174
North America 20.28%	729
Oceania 7.31%	260

Q22 HOW LIKELY ARE THE FOLLOWING REGIONS TO USE GDPR AS A MODEL FOR CRAFTING DATA PRIVACY LEGISLATION OR REGULATIONS IN THE NEXT 3-5 YEARS?

Very likely	Responses
Africa 6.77%	242
Asia 16.81%	600
Latin America 11.01%	390
Middle East 11.27%	398
North America 31.24%	1115
Oceania 17.23%	611




Q23 IN WHICH REGION DO YOU LIVE?

Answer Choices	Responses
Africa 5.69%	287
Asia 16.10%	812
Europe 27.69%	1397
Latin America 3.51%	177
Middle East 2.60%	131
North America 40.91%	2064
Oceania 3.51%	177
	Answered 5045
	Skipped 480









Q25 WHICH OF THE FOLLOWING, IF ANY, BEST DESCRIBES YOUR BUSINESS CATEGORY?

Answer Choices		Responses
Financial/Banking	23.49%	1185
Insurance	5.79%	292
Public Accounting	4.24%	214
Transportation	2.06%	104
Aerospace	0.34%	17
Retail/Wholesale/Distribution	3.41%	172
Government/Military—National/State/Local	8.74%	441
Technology Services/Consulting	23.29%	1175
Manufacturing/Engineering	5.07%	256
Telecommunications/Communications	3.73%	188
Mining/Construction/Petroleum/Agriculture	2.22%	112
Utilities	1.76%	89
Legal/Law/Real Estate	0.83%	42
Healthcare/Medical	4.10%	207
Pharmaceutical	1.11%	56
Advertising/Marketing/Media	1.19%	60
Other	8.62%	435
	Answered	5045
	Skipped	480

Q26 DOES YOUR ORGANIZATION HAVE AN EXECUTIVE OFFICER RESPONSIBLE FOR DATA PRIVACY PROTECTION (E.G. A DPO)?

Answer Choices		Responses
Yes	 60.46%	3050
No	 28.82%	1454
Don't know	 10.72%	541
	Answered	5045
	Skipped	480

Q27 HOW MANY EMPLOYEES DOES YOUR ORGANIZATION HAVE IN TOTAL, INCLUDING ALL LOCATIONS?

Answer Choices		Responses
Fewer than 50 employees	 9.32%	470
50 – 149 employees	 6.38%	322
150 – 499 employees	 9.26%	467
500 – 1,499 employees	 12.61%	636
1,500 – 4,999 employees	 15.84%	799
5,000 – 9,999 employees	 9.02%	455
10,000 – 14,999 employees	 5.49%	277
15,000 or more employees	 32.09%	1619
	Answered	5045
	Skipped	480

Q29 WHICH OF THE FOLLOWING BEST DESCRIBES YOUR PRIMARY JOB RESPONSIBILITIES?

Answer Choices		Responses
Audit / Assurance	32.75%	1652
Risk	5.79%	512
Compliance	4.24%	518
Security	2.06%	1120
Privacy	0.34%	57
IT Strategy/Governance	3.41%	680
Student	8.74%	1
Academic Faculty	23.29%	12
Retired	5.07%	10
Unemployed	3.73%	9
Other IT role	2.22%	303
Other	8.62%	171
	Answered	5045
	Skipped	480

Data Protection That Works: Getting to **GDPR** compliance

Establish a more secure and integrated data security program that meets the productivity needs of your employees, the compliance requirements of your industry, and your own evolving data security needs.

Bring your data protection policies and programs to life within your existing security environment by leveraging the most configurable policy administration platform.

Policies (and regulations) change. TITUS will help you centrally manage these changes so you can quickly adapt to, and adopt, new security requirements.

TITUS data protection solutions enable you to protect what matters while ensuring people, process and technology can work together. For over 12 years, millions of users in 120 countries have leveraged TITUS to identify and secure their sensitive data.

How does TITUS support GDPR compliance?



Processing personal data

Identify personal data, including special categories – at creation, at rest and in motion.



Data protection and privacy by design

With the most flexible and powerful policy engine, drive the policies for your data security stack with TITUS-embedded metadata.



Ongoing awareness and compliance

Build a security mindset to promote protection of personal data in the flow of work.

TITUS works where your employees work – across multiple products and platforms.

Find out more at titus.com.