The Race to GDPR:

A Study of Companies in the United States & Europe

Sponsored by McDermott Will & Emery LLP

Independently conducted by Ponemon Institute LLC

Publication Date: April 2018

Ponemon INSTITUTE

McDermott Will & Emery

THE RACE TO GDPR:
A STUDY OF COMPANIES IN THE UNITED STATES & EUROPE

PONEMON INSTITUTE, APRIL 2018

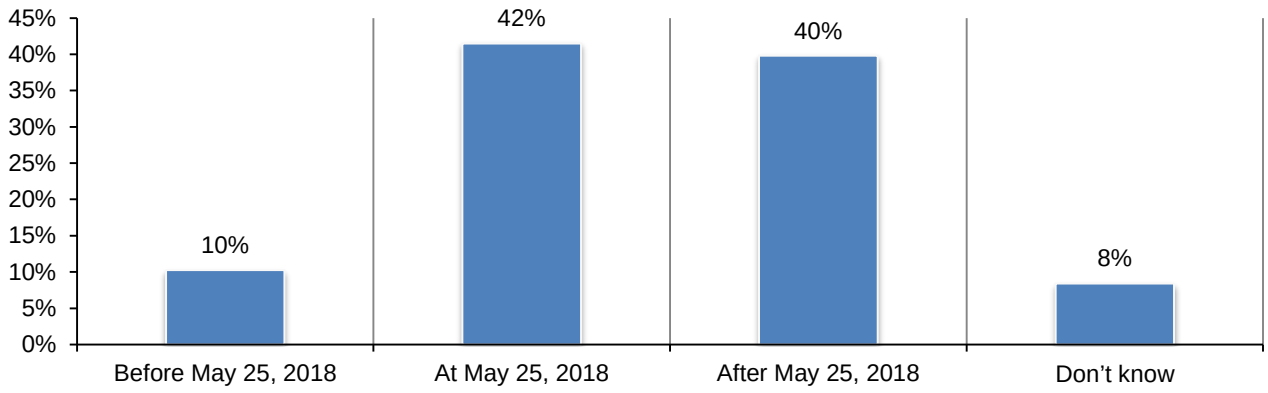
Part 1. Introduction

The race to achieve compliance with the European Union's (EU) General Data Protection Regulation (GDPR) is nearing its final lap and is scheduled to go into effect May 25, 2018. Many companies in both in the US and EU admit they are behind schedule in implementing the privacy and security processes needed to ensure they meet the regulation's requirements and obligations.

More than 1,000 companies in the United States and European Union are represented in *The Race to GDPR*, sponsored by McDermott Will and Emery LLP[1]. Participants in this research work in a variety of departments including IT, IT security, compliance, legal, data protection office and privacy. Ninety percent of respondents say their company is subject to GDPR[2] and 10 percent are unsure.

Almost half of companies represented in this research will not meet the May 25 deadline or don't know. Respondents say that compared to other regulations compliance with GDPR is either more or equally difficult to comply with. As shown in Figure 1, 40 percent of respondents say they will achieve compliance *after* May 25, and 8 percent do not know when they will achieve compliance.

FIGURE 1. WHEN DO YOU EXPECT TO BE IN COMPLIANCE WITH GDPR?



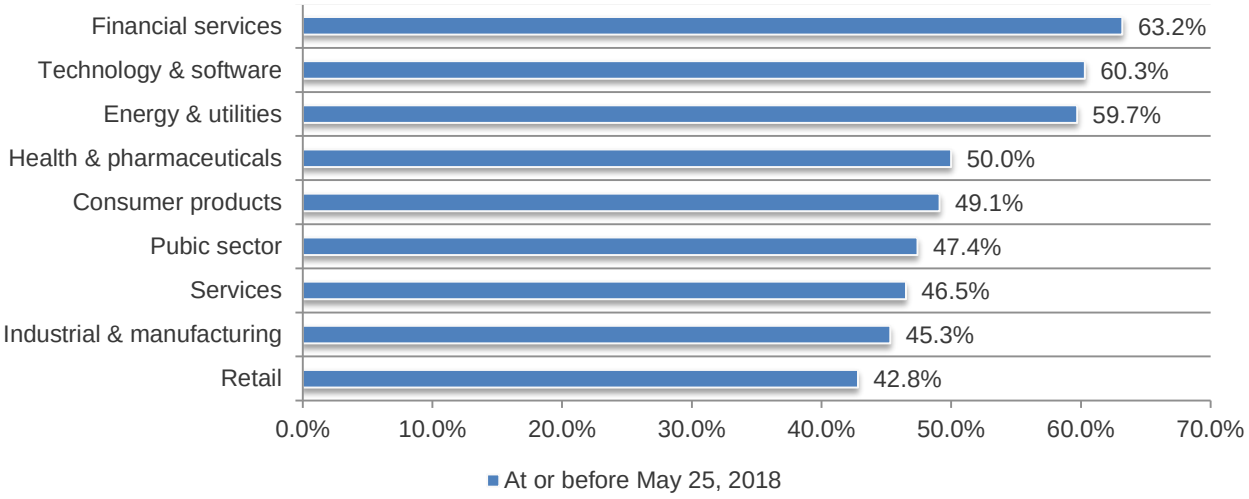
[1] Ponemon Institute and McDermott Will & Emery are appreciative of Sam Pfeifle, Content Director, IAPP, for his time and valuable contributions to this research study.

[2] The new **General Data Protection Regulation** (GDPR) is set to replace the Data Protection Directive 95/46/ec, effective May 25, 2018. The GDPR is directly applicable in each EU member state, as well as in countries outside the EU. It also addresses export of personal data outside the EU. Personal data is defined as any information relating to an identified or identifiable natural person (data subject). Under the GDPR, a "personal data breach" is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."

Industry sector and company size are important factors in GDPR readiness. As can be seen, financial service organizations report the highest readiness level, followed by companies in technology and software and energy and utilities. In contrast, companies in retail, industrial manufacturing and services report the lowest readiness level.

FIGURE 2. INDUSTRY EFFECTS: WHEN DO YOU EXPECT YOUR ORGANIZATION WILL BE SATISFIED WITH ITS EFFORTS TO BE IN COMPLIANCE WITH GDPR?

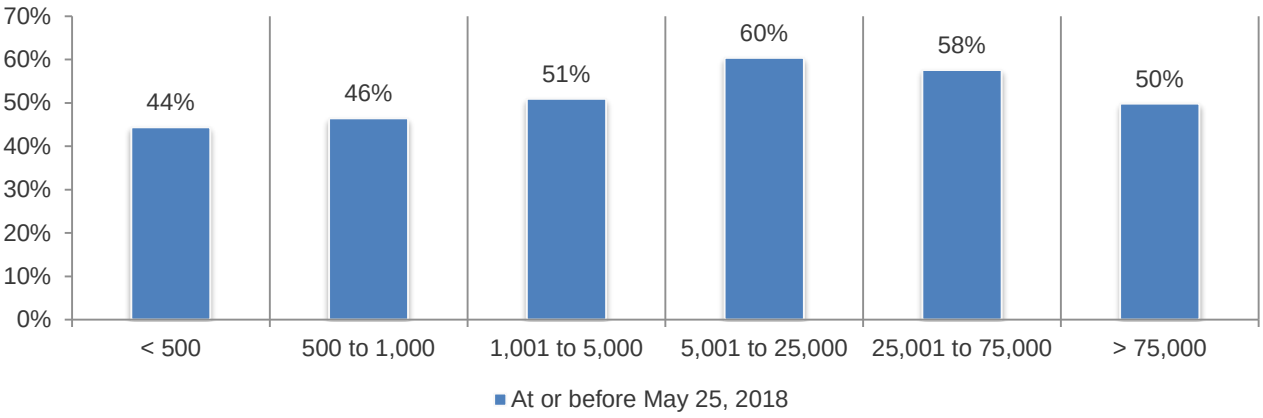
Following are the averages for nine (9) industries with respect to the selection "When do you expect to be in compliance with GDPR – At or before May 25, 2015." The overall mean is 52 percent.



Smaller companies and very large companies see themselves as less likely to be in compliance with GDPR by the effective date than do mid-size companies. Figure 3 reveals an inverted U-shaped relationship between GDPR readiness and organizational size. As can be seen, smaller-sized organizations report the lowest readiness level, while companies with 5,000 to 25,000 employees report the highest readiness level. Large companies with more than 25,000 employees have a lower level of readiness than middle-sized organizations.

FIGURE 3. SIZE EFFECTS: WHEN DO YOU EXPECT YOUR ORGANIZATION WILL BE SATISFIED WITH ITS EFFORTS TO BE IN COMPLIANCE WITH GDPR?

Following are the averages for six (6) organizational size (headcount) ranges with respect to the selection "When do you expect to be in compliance with GDPR – At or before May 25, 2015." The overall mean is 52 percent.



Part 2. Key findings

In this section we provide an analysis of the research. Unless indicated otherwise, we present the consolidated findings for the US and EU. A special section, as noted below, will describe the most salient differences between respondents in the US and EU. The complete audited findings are presented in the Appendix of the report. We have organized the report according to the following topics.

- The impact of GDPR on business practices
- The state of readiness to comply with data breach notification obligations
- The risk of non-compliance
- GDPR's future impact on companies
- The GDPR budget
- A comparison of US and EU respondents

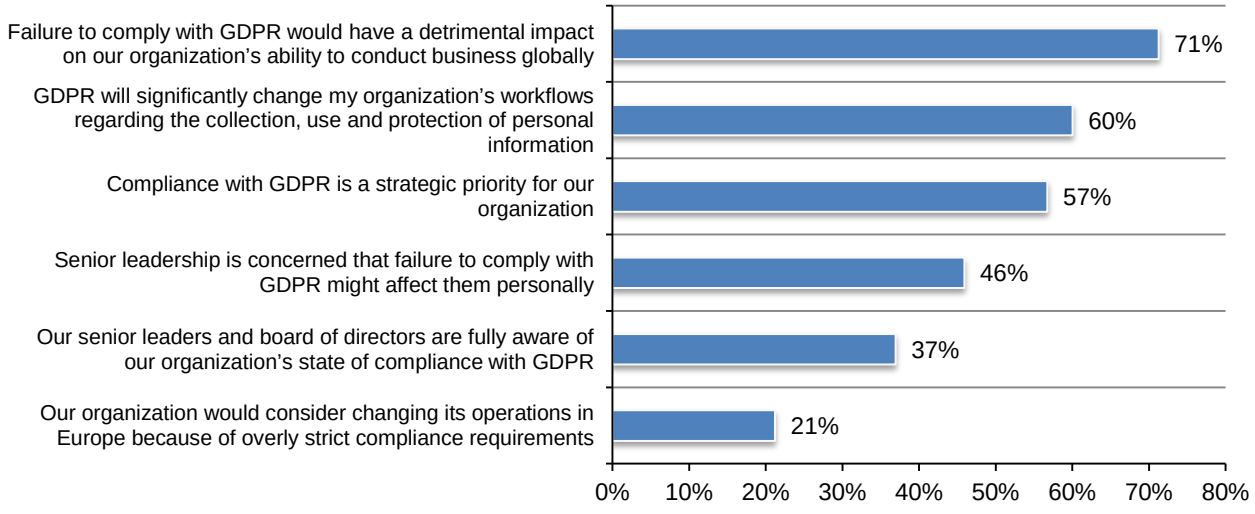
THE IMPACT OF GDPR ON BUSINESS PRACTICES

Compliance with GDPR is considered critical but daunting. GDPR is expected to compel companies to make significant changes in their global operations. As shown in Figure 4, 71 percent of respondents say that failure to comply with GDPR would have a detrimental impact on their organizations' ability to conduct business globally and 60 percent of respondents say it will significantly change workflows regarding the collection, use and protection of personal information. Despite their issues in achieving compliance, only 21 percent of respondents say their organizations would change their operations because of the overly strict compliance requirements.

Respondents believe GDPR will have a significant impact on their companies' operations and 57 percent of respondents say compliance is a strategic priority. However, only 37 percent of respondents say their senior leaders and board of directors are fully aware of their organizations' state of compliance with GDPR.

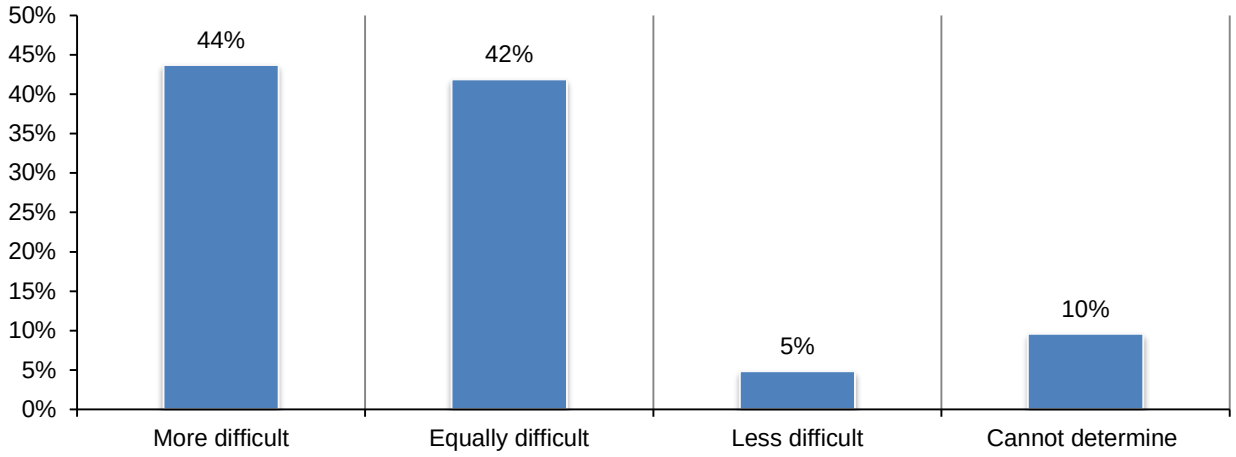
FIGURE 4. PERCEPTIONS ABOUT THE IMPORTANCE OF COMPLIANCE WITH GDPR

Strongly agree and Agree responses combined



Compliance with GDPR is more difficult than, or as difficult as meeting other privacy and security requirements. According to Figure 5, 86 percent of respondents say compliance with GDPR is more difficult (44 percent) or equally difficult (42 percent).

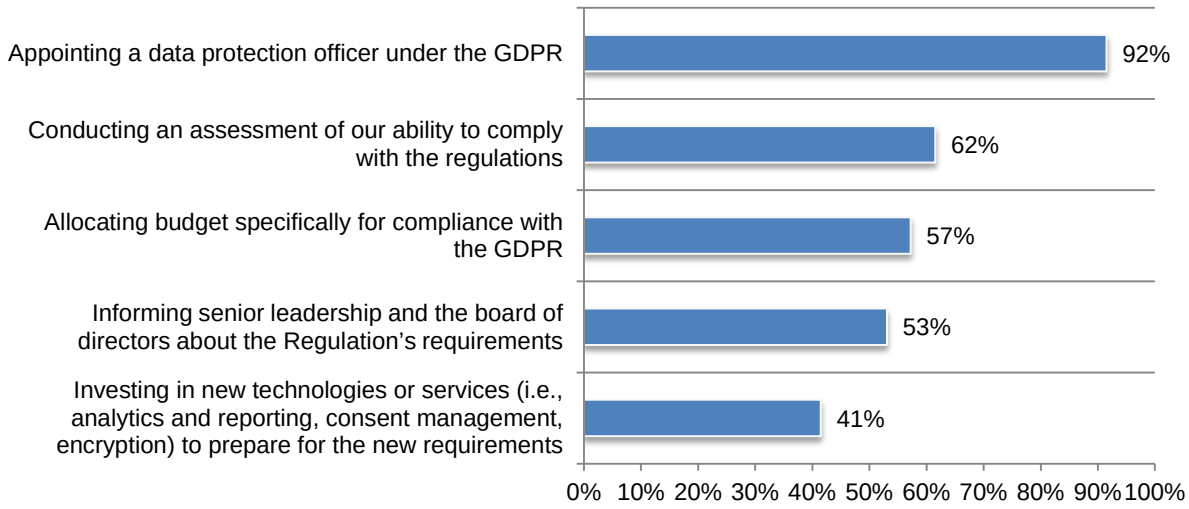
FIGURE 5. RELATIVE TO OTHER DATA PRIVACY AND SECURITY REQUIREMENTS, HOW DIFFICULT WILL THE GDPR BE TO IMPLEMENT?



Many companies do not understand what is required to be in compliance. Forty-seven percent of respondents do not know where to begin their path to compliance. Of the 53 percent of respondents who understand compliance requirements, 92 percent say their organizations have appointed a data protection officer and 62 percent of respondents report their companies are conducting an assessment of their ability to comply with regulations, as shown in Figure 6.

FIGURE 6. HOW IS YOUR COMPANY PREPARING FOR COMPLIANCE WITH GDPR?

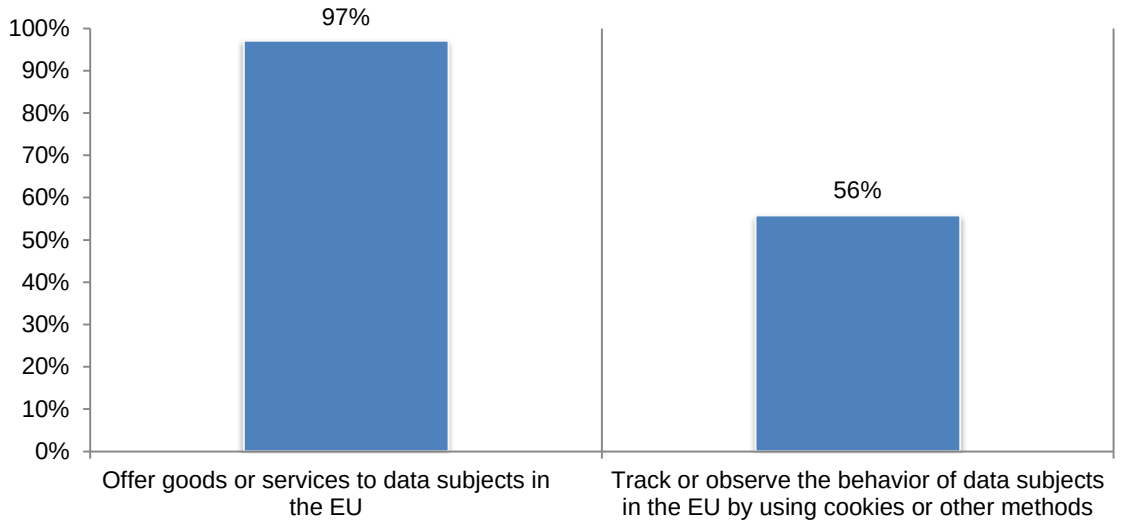
More than one response allowed



Who has to comply with GDPR? Companies are required to comply with GDPR if they offer goods or services or track data subjects in the EU. As shown in Figure 7, 97 percent of respondents say their organizations offer goods or services to EU data subjects for sale or for free and 56 percent of respondents say their companies track or observe the behavior of data subjects in the EU by using cookies or other methods.

FIGURE 7. WHAT ARE THE PRACTICES OF COMPANIES IN THE EU?

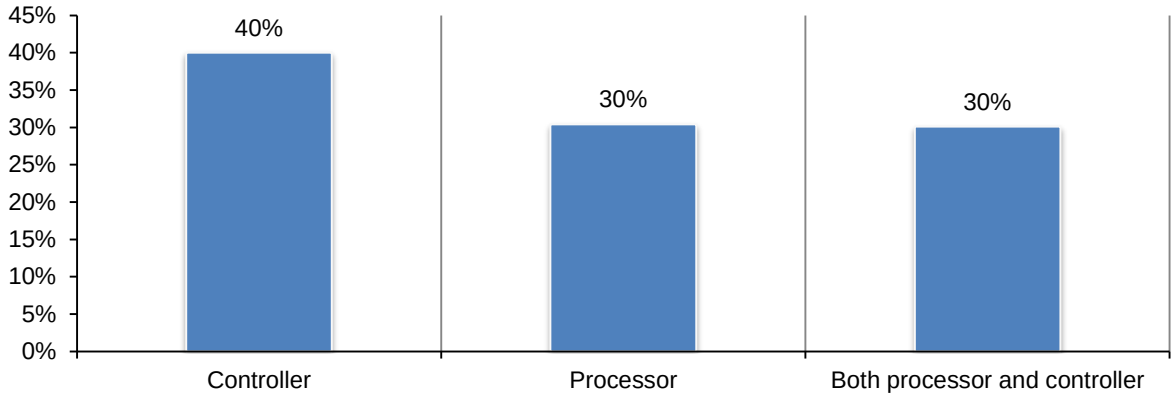
Yes responses



Most companies represented in this study are controllers. Under GDPR, the controller determines the purposes and means of the processing of personal data from customers and third parties based on EU or Member State law. The processor processes personal data on behalf of the controller.

As shown in Figure 8, 40 percent of respondents say their companies are controllers, 30 percent of respondents say they are processors and another 30 percent of respondents say their organizations are both. In their efforts to comply with GDPR, 37 percent of processors say they will change their status to controller.

FIGURE 8. WHAT DO YOU CONSIDER YOUR ORGANIZATION TO BE?



According to Figure 9, common practices of companies represented in this study are call centers and customer service operations (91 percent of respondents), sales management (87 percent of respondents) and advertising and promotion campaigns (87 percent of respondents).

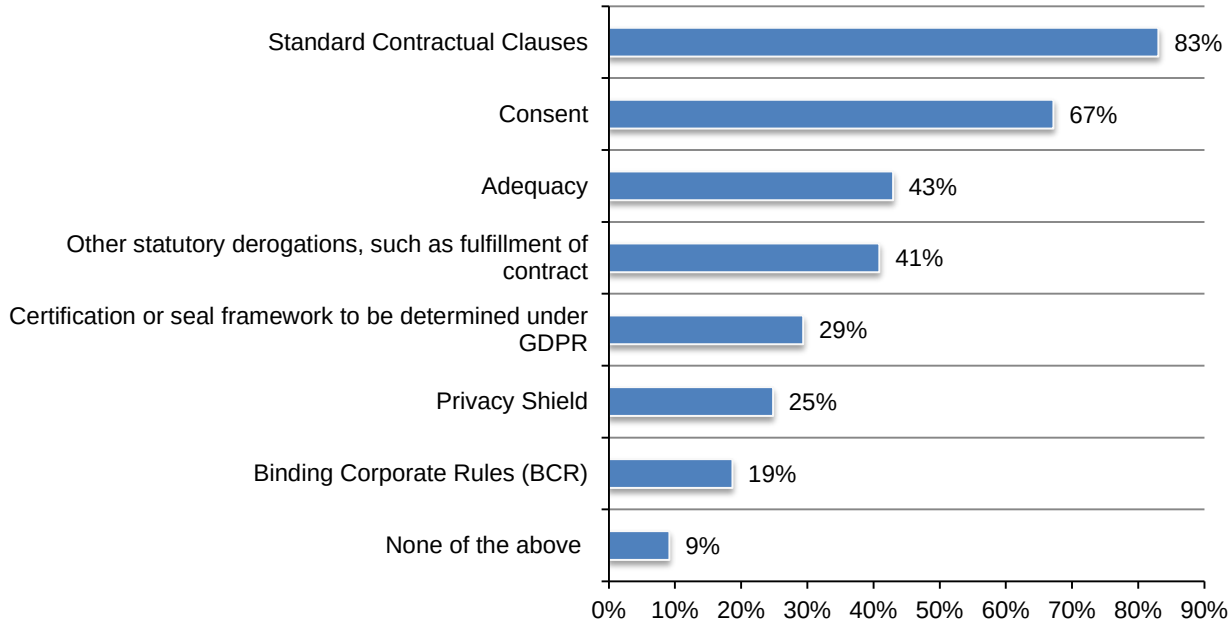
FIGURE 9. WHAT PRACTICES DOES YOUR ORGANIZATION CONDUCT WITH YOUR OFFICES AND THIRD PARTIES THROUGHOUT THE WORLD?

More than one response allowed

Currently, companies use a variety of mechanisms to transmit EU personal data outside of the EU. Eighty-three percent of respondents say their companies use Standard Contractual Clauses to transmit EU personal data outside of the EU. This is followed by consent (67 percent of respondents), adequacy (43 percent of respondents) and other statutory derogations, such as fulfillment of contract (41 percent of respondents), as shown in Figure 10.

FIGURE 10. MECHANISMS USED TO TRANSMIT EU PERSONAL DATA OUTSIDE OF THE EU

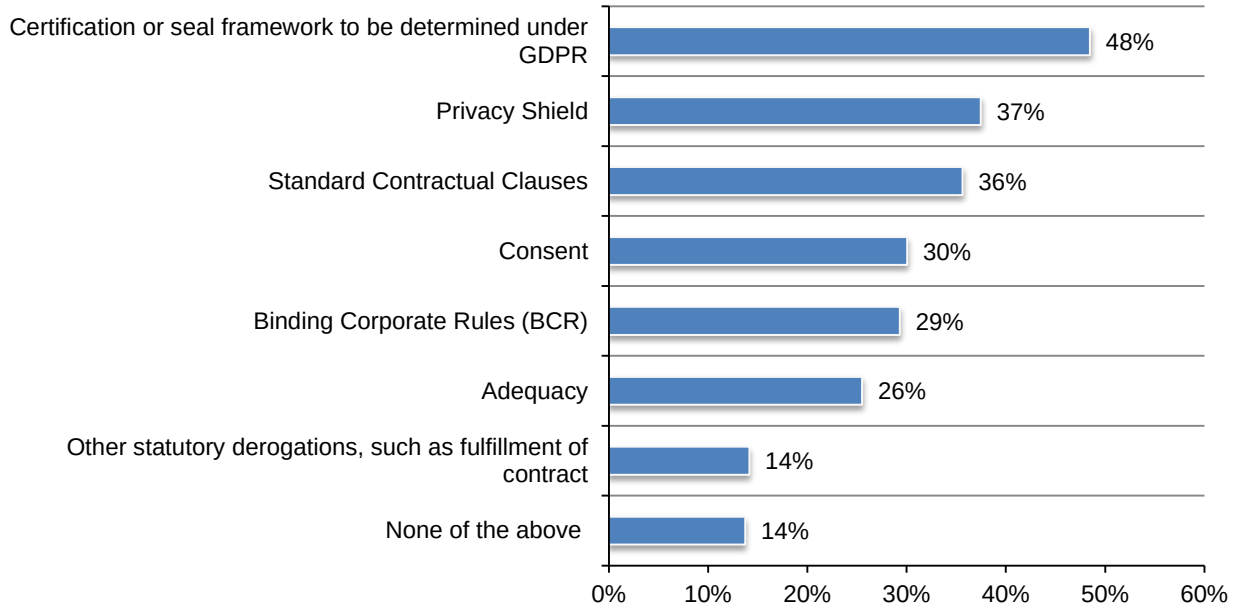
More than one response allowed



Forty-six percent of the respondents above say that after May 25, they will consider changing the mechanism they use to transfer EU data out of the EU. Almost half of that 46 percent say they will consider changing to a certification or seal framework to be determined under GDPR. As shown in Figure 11, companies are considering changing their current mechanism to Privacy Shield (37 percent) and Standard Contractual Clauses (36 percent).

FIGURE 11. WHICH MECHANISMS WILL YOUR ORGANIZATION CHANGE TO?

More than one response allowed



THE STATE OF READINESS TO COMPLY WITH DATA BREACH NOTIFICATION OBLIGATIONS

Following are the GDPR obligations defined in the survey.

Notice: In the event of a personal data breach, the data controllers must notify the supervisory authority within 72 hours. If there is a delay, the controller must provide a "reasoned justification."

Right to Access: The right for data subjects to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. Further the controller shall provide a copy of the personal data, free of charge, in an electronic format.

Right to Be Forgotten: Entitles the data subject to have the data controller erase his or her personal data, cease further dissemination of the data and potentially have third parties halt processing the data.

Data Portability: The right for a data subject to receive the personal data concerning them, which they have previously provided in a *commonly used and machine readable format* and have the right to transmit that data to another controller.

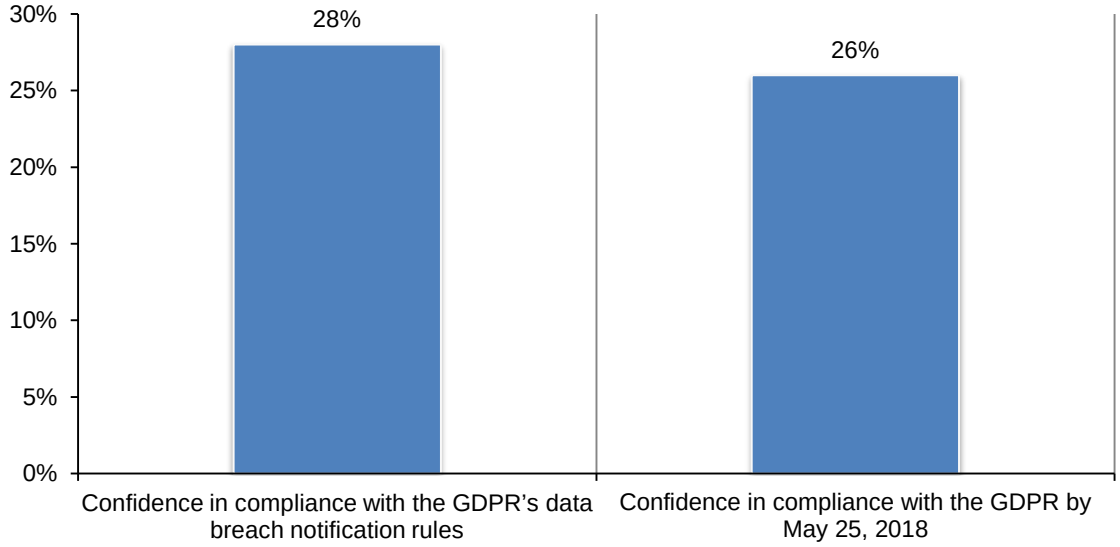
Privacy by Design: The inclusion of data protection from the onset of the designing of systems, rather than an addition.

Data Protection Officer (DPO): A DPO is mandatory for those controllers and processors whose core activities consist of processing operations that require regular and systematic monitoring of data subjects on a large scale or of special categories of data or data relating to criminal convictions and offenses.

Confidence in meeting the deadline and data breach notification rules is low. Respondents were asked to rank their confidence in complying with GDPR's data breach notification laws and with GDPR on a scale of 1 = low confidence to 10 = high confidence. Figure 12 shows that only 26 percent have a high level of confidence in meeting the deadline and only 28 percent are confident in their ability to comply with the data breach notification rules.

FIGURE 12. CONFIDENCE IN COMPLIANCE BY MAY 25, 2018 AND IN COMPLIANCE WITH DATA BREACH NOTIFICATION RULES

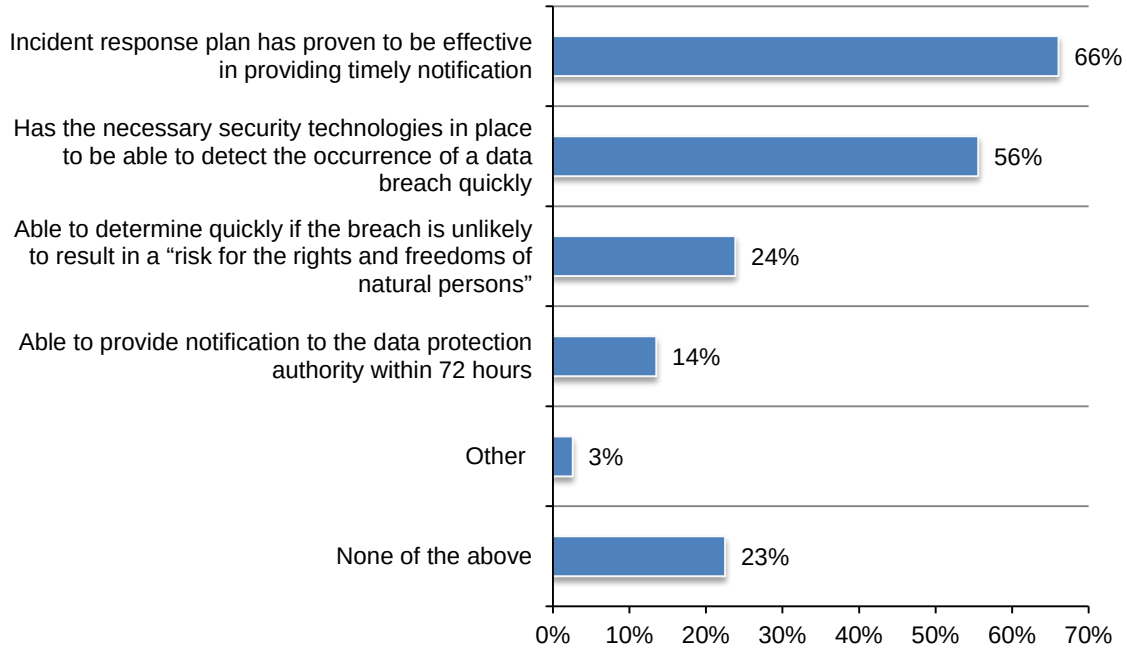
1 = low confidence to 10 = high confidence, 7+ responses combined



Incident response plans that have proven to be effective are important to achieving compliance with the GDPR's data breach notification rules. Of the 28 percent of respondents who say their organizations are highly confident in their ability to comply with the GDPR's data breach notification rules, it is because their organizations' incident response plans result in providing timely notification (66 percent of respondents) or they have the necessary security technologies in place to be able to detect the occurrence of a data breach quickly (56 percent of respondents), as shown in Figure 13.

FIGURE 13. IF CONFIDENT IN COMPLIANCE WITH THE GDPR'S DATA BREACH NOTIFICATION RULES, WHY?

More than one response allowed



A data breach would have severe financial consequences. If their companies had a data breach, 53 percent of respondents believe fines would be the worst consequence followed by other significant financial harms, as shown in Figure 14.

FIGURE 14. WHAT CONSEQUENCES OF A DATA BREACH ARE YOU MOST CONCERNED ABOUT?

Three responses allowed

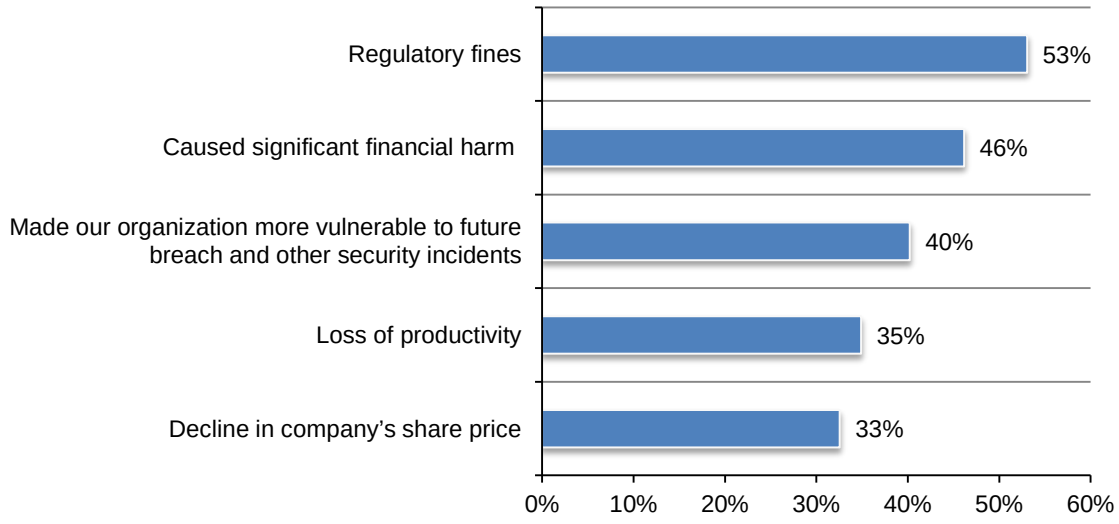
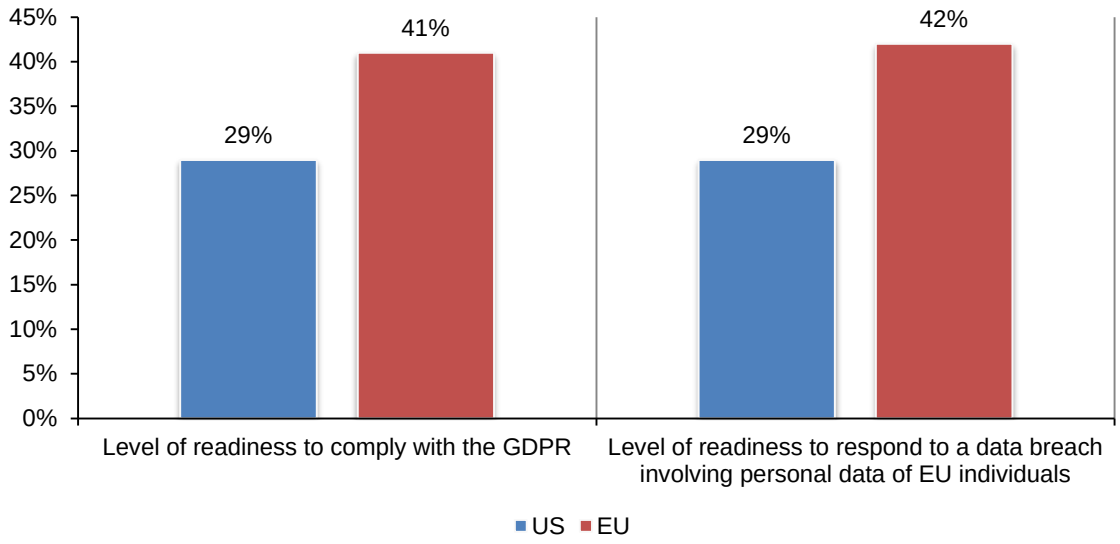


Figure 15 presents the findings of those respondents who report a high level of readiness (7+ on the scale of 1 to 10) to comply with the GDPR and respond to a EU data breach. Only 29 percent of US respondents say they are very ready to comply with the GDPR and respond to a EU data breach. While still low, more respondents in Europe believe they will achieve compliance with GDPR (41 percent of respondents) and, in the event it occurs, are ready to respond to a EU data breach (42 percent of respondents).

FIGURE 15. ARE COMPANIES READY TO COMPLY WITH GDPR AND RESPOND TO A EU DATA BREACH?

7+ on a scale of 1 = low readiness to 10 = high readiness

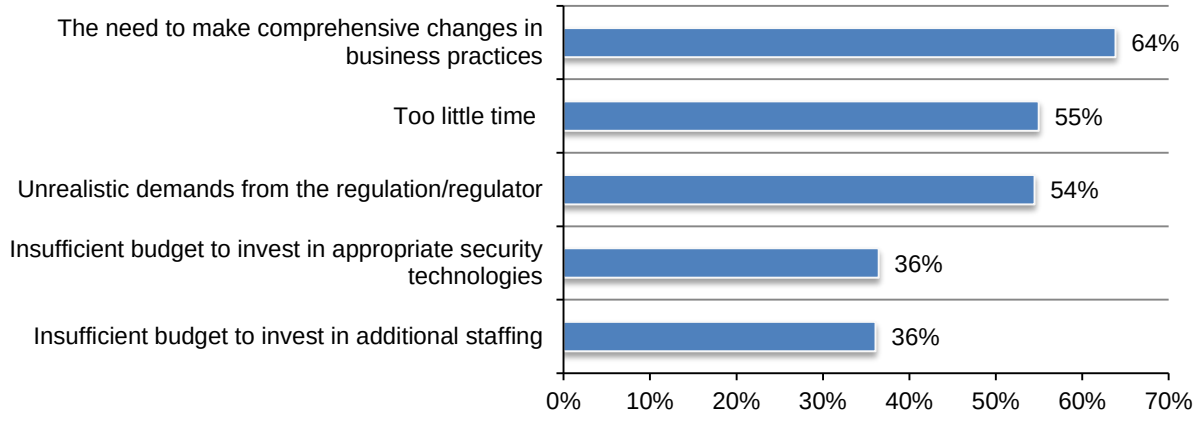


The need to make comprehensive changes to business practices is the biggest barrier to compliance. As previously discussed, 60 percent of respondents recognize that GDPR will significantly change their organizations' workflows regarding the collection, use and protection of personal information.

As shown in Figure 16, 64 percent of respondents say they are concerned about the need to make comprehensive changes in business practices before achieving compliance. Fifty-five percent of respondents say there is too little time and 54 percent of respondents say regulators and the regulation have unrealistic demands.

FIGURE 16. WHAT ARE THE BARRIERS TO GDPR COMPLIANCE?

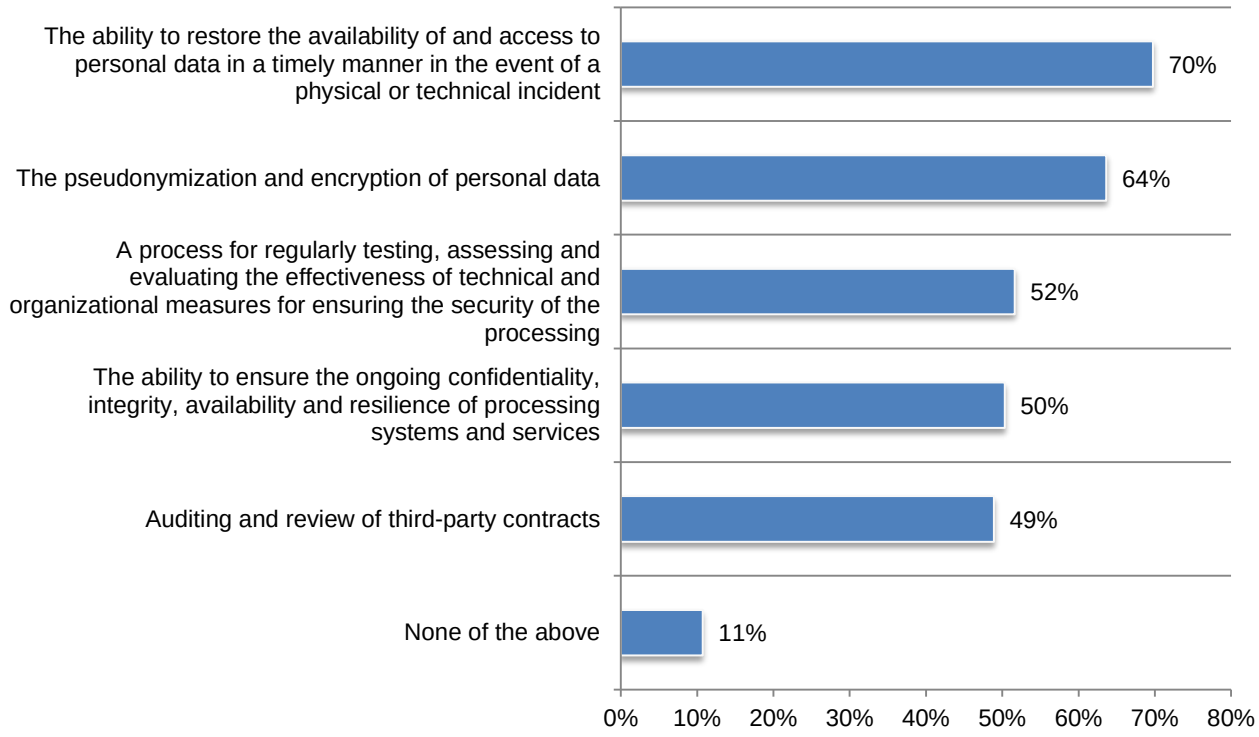
Three responses allowed



GDPR calls for specific security actions to be in place. As shown in Figure 17, 70 percent of respondents say they are able to restore the availability of and access to personal data in a timely manner in the event of a physical or technical incident, and 64 percent of respondents say their organizations are prepared to pseudonymize and encrypt personal data.

FIGURE 17. WHICH OF THE FOLLOWING SECURITY ACTIONS IN GDPR IS YOUR ORGANIZATION PREPARED TO ADDRESS?

More than one response allowed



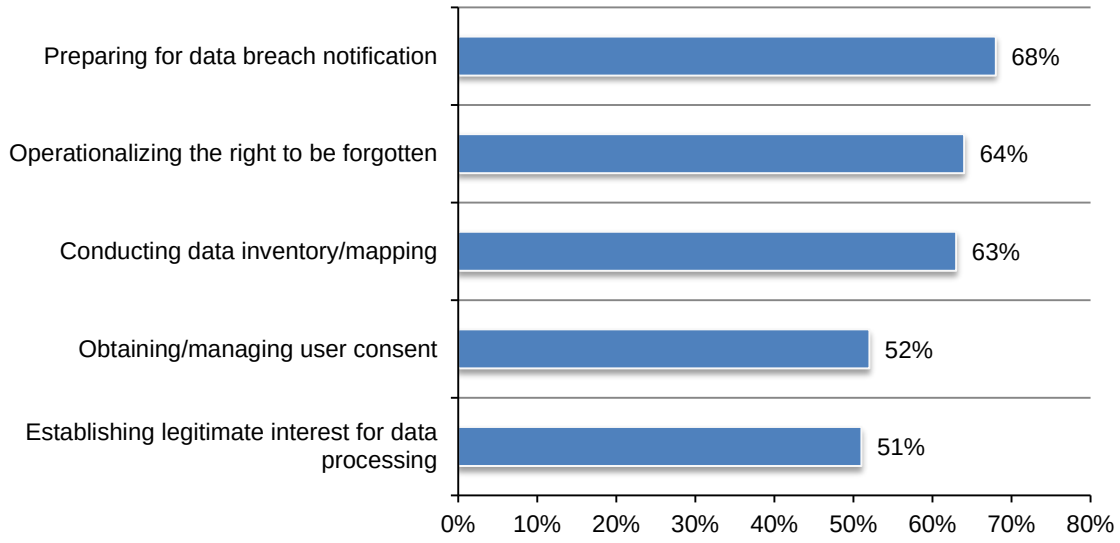
THE RISK OF NON-COMPLIANCE

Companies are concerned about the risk of noncompliance with certain GDPR obligations. Eighty-four percent of respondents believe their organizations are at greater risk for potential fines and regulatory action because of their profile with regulators. They also believe their organizations are at a high risk if they fail to comply with specific GDPR obligations.

Respondents were asked to rank each obligation on a scale of low to high risk: 1 being low and 10 being high. Figure 18 shows the five GDPR obligations respondents believe pose the greatest risk for fines and regulatory action (7+ on a scale of 1 to 10) if they are not in compliance. These are: preparing for data breach notification (68 percent of respondents), operationalizing the right to be forgotten (64 percent of respondents), conducting data inventory/mapping (63 percent of respondents), obtaining/managing user consent (52 percent of respondents) and establishing legitimate interest for data processing (51 percent of respondents).

FIGURE 18. THE GDPR OBLIGATIONS THAT POSE THE GREATEST RISK IF NOT IN COMPLIANCE

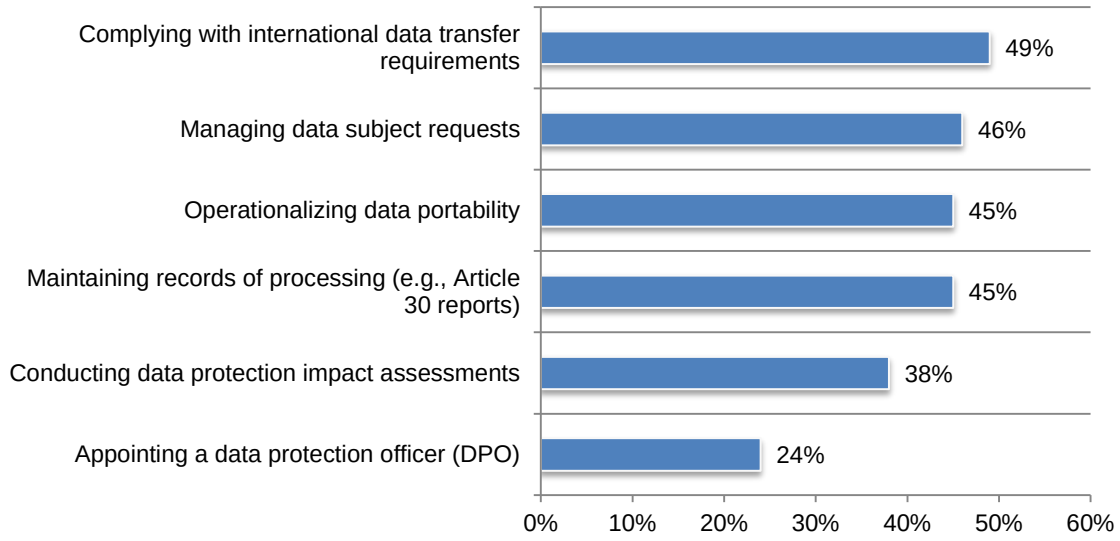
1 = low risk to 10 = high risk, 7+ responses combined


Preparing for data breach notification
68%
Operationalizing the right to be forgotten
64%
Conducting data inventory/mapping
63%
Obtaining/managing user consent
52%
Establishing legitimate interest for data processing
51%
0%
10%
20%
30%
40%
50%
60%
70%
80%

Fewer respondents rate the GDPR obligations presented in Figure 19 as posing a high risk. These are: complying with international data transfer requirements (49 percent of respondents), managing data subject requests (46 percent of respondents), operationalizing data portability (45 percent of respondents), maintaining records of processing (*e.g.*, Article 30 reports) (45 percent), conducting data protection impact assessments (38 percent of respondents) and appointing a DPO (24 percent of respondents)

FIGURE 19. THE GDPR OBLIGATIONS THAT POSE LESS OF A RISK IF NOT IN COMPLIANCE

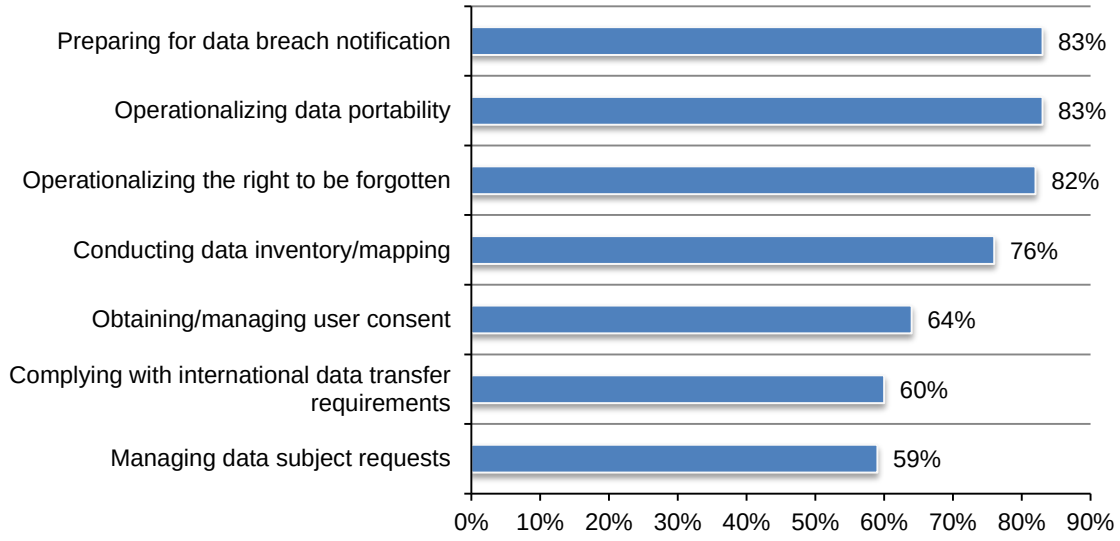
1 = low risk to 10 = high risk, 7+ responses combined



Data breach notification and data portability are the most difficult obligations to comply with. Respondents were asked to rate compliance with GDPR obligations on a scale of 1 = low difficulty to 10 = high difficulty. According to Figure 20, 83 percent of respondents say preparing for data breach notification and operationalizing data portability are the most difficult of all GDPR obligations. However, as shown above, the risk associated with data portability is not as high as other obligations. Operationalizing the right to be forgotten is also very difficult according to 82 percent of respondents.

FIGURE 20. THE MOST DIFFICULT GDPR OBLIGATIONS TO COMPLY WITH

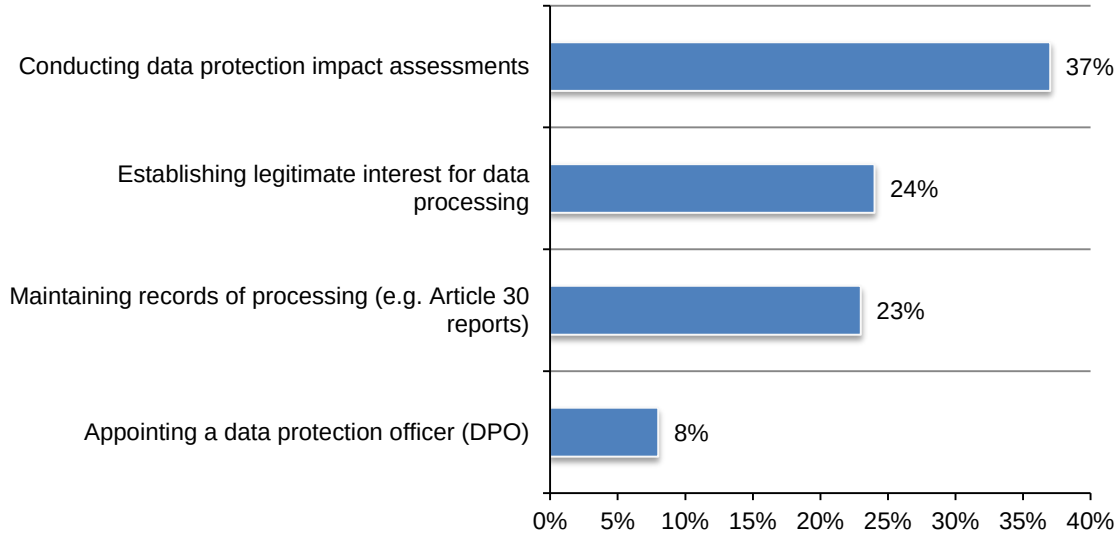
1 = low difficulty to 10 = high difficulty, 7+ responses combined



Fewer respondents rate conducting data protection impact assessments as difficult. As shown in Figure 21, only 37 percent of respondents rate conducting data protection impact assessments as very difficult. Only 8 percent indicate the appointment of a DPO as very difficult.

FIGURE 21. THE LEAST DIFFICULT GDPR OBLIGATIONS TO COMPLY WITH

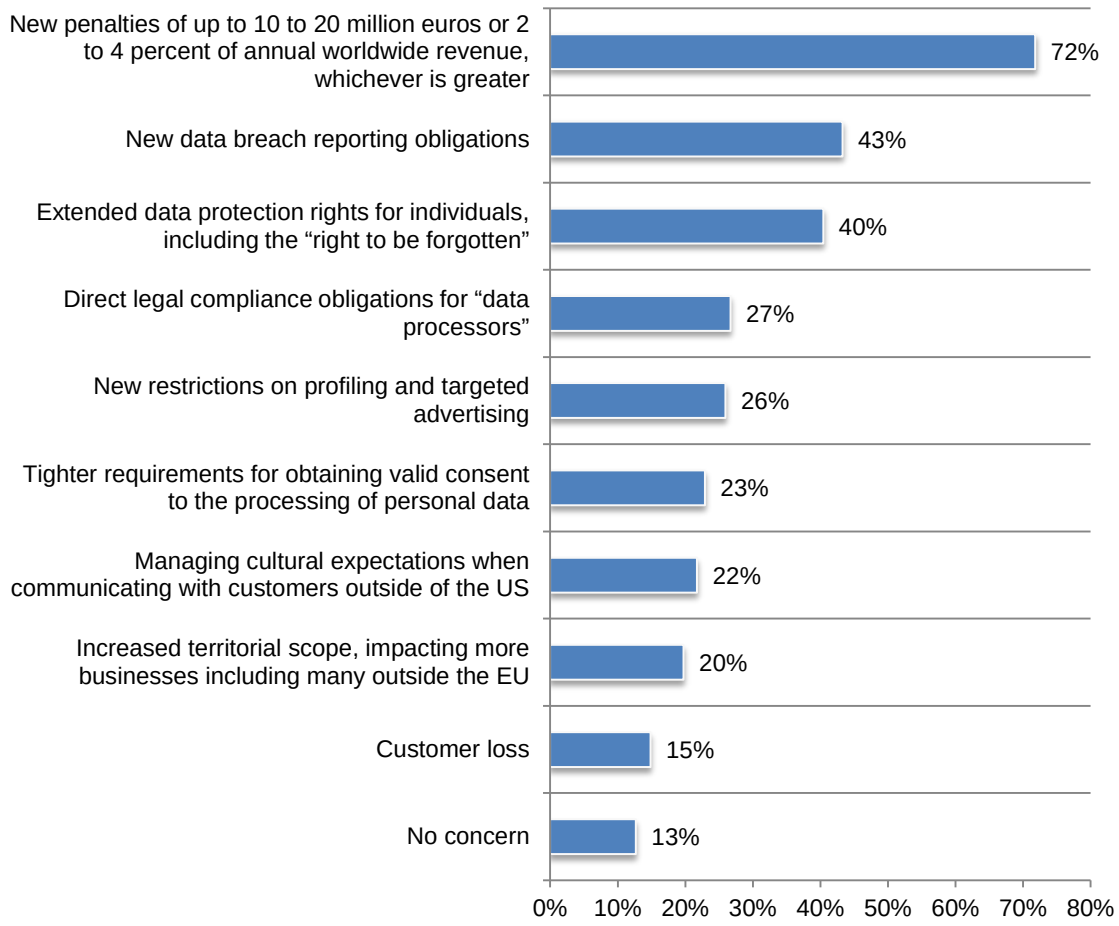
1 = low difficulty to 10 = high difficulty, 7+ responses combined



Companies are most concerned about the risk of incurring financial penalties. As shown in Figure 22, 72 percent of respondents are most worried about the financial penalties if their companies are found in noncompliance. This is followed by the new data breach reporting obligations and extended data protection rights for individuals, including the "right to be forgotten," according to 43 percent and 40 percent of respondents, respectively.

FIGURE 22. WHAT ARE YOUR TOP CONCERNS ABOUT NON-COMPLIANCE WITH GDPR?

Three responses allowed

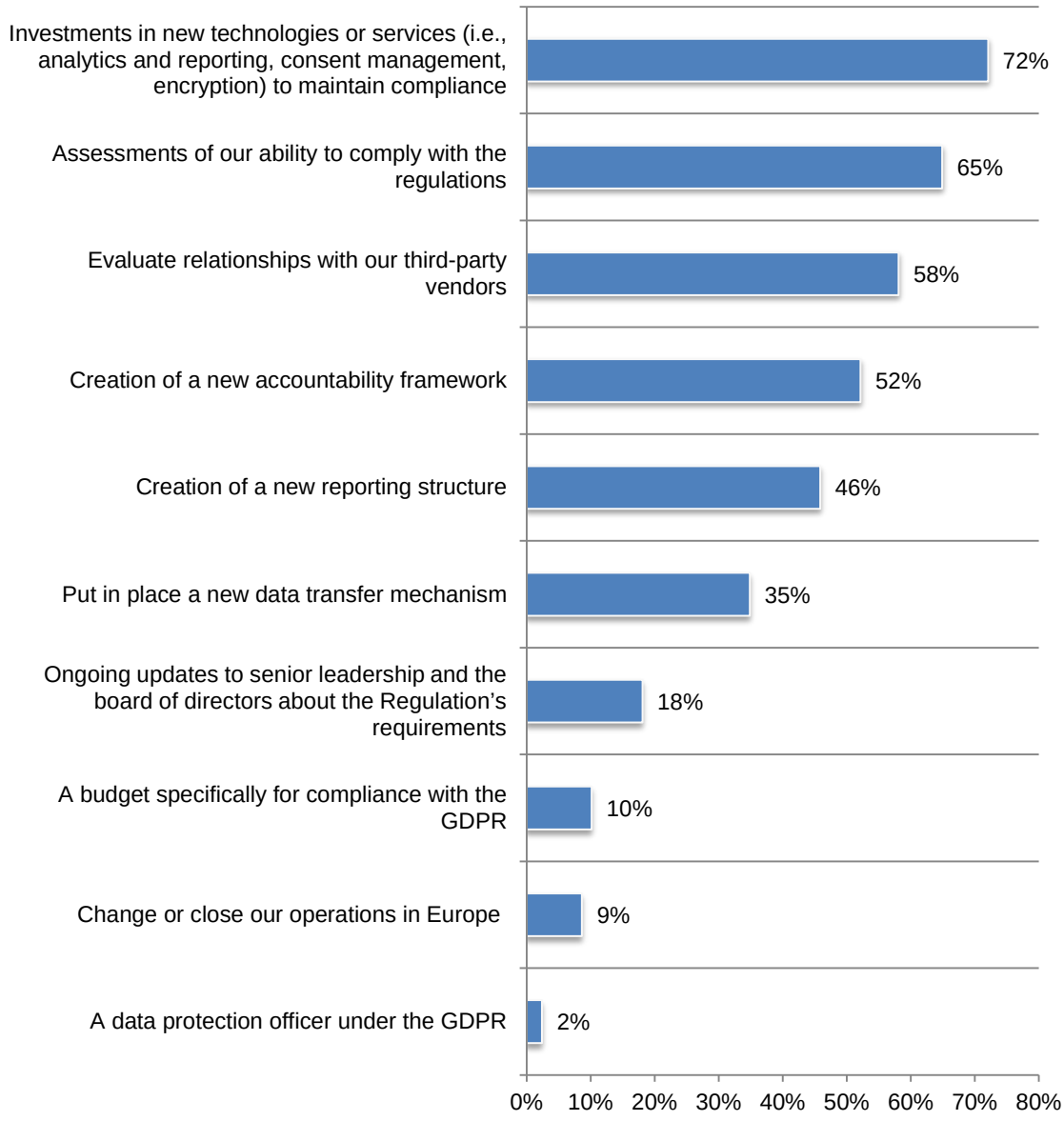


GDPR'S FUTURE IMPACT ON COMPANIES

GDPR will require ongoing investments in technologies and governance practices. As shown in Figure 23**,** 72 percent of respondents say their organizations will have to make investments in new technologies or services (*i.e.*, analytics and reporting, consent management, encryption) to maintain compliance. Other ongoing practices will include assessments of the ability to comply with regulations (65 percent of respondents), evaluation of relationships with third-party vendors (58 percent of respondents) and the creation of a new accountability framework (52 percent of respondents).

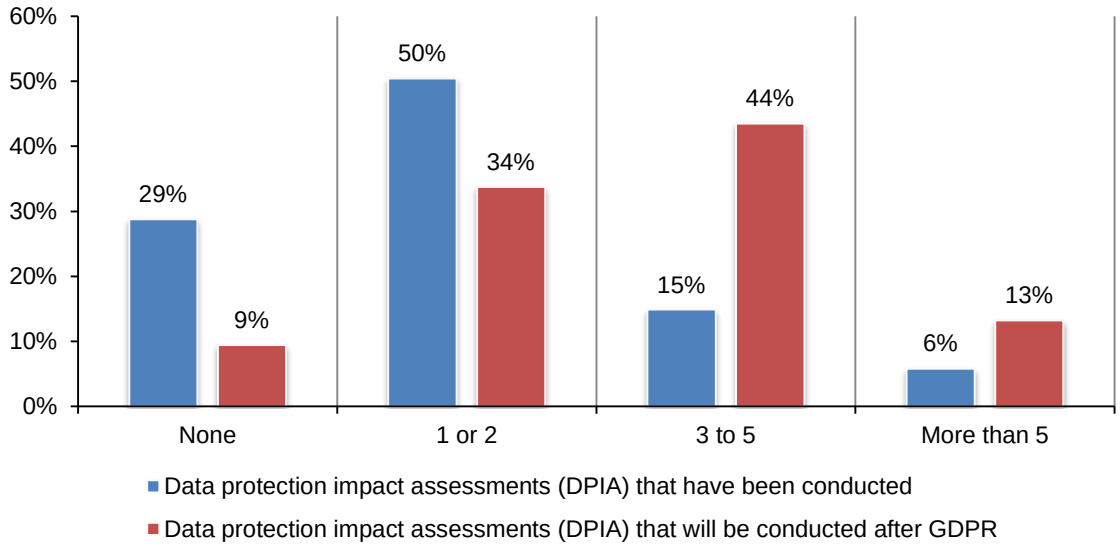
FIGURE 23. WHICH OF THE FOLLOWING AREAS WILL REQUIRE SIGNIFICANT EFFORTS AFTER MAY 25?

More than one response permitted



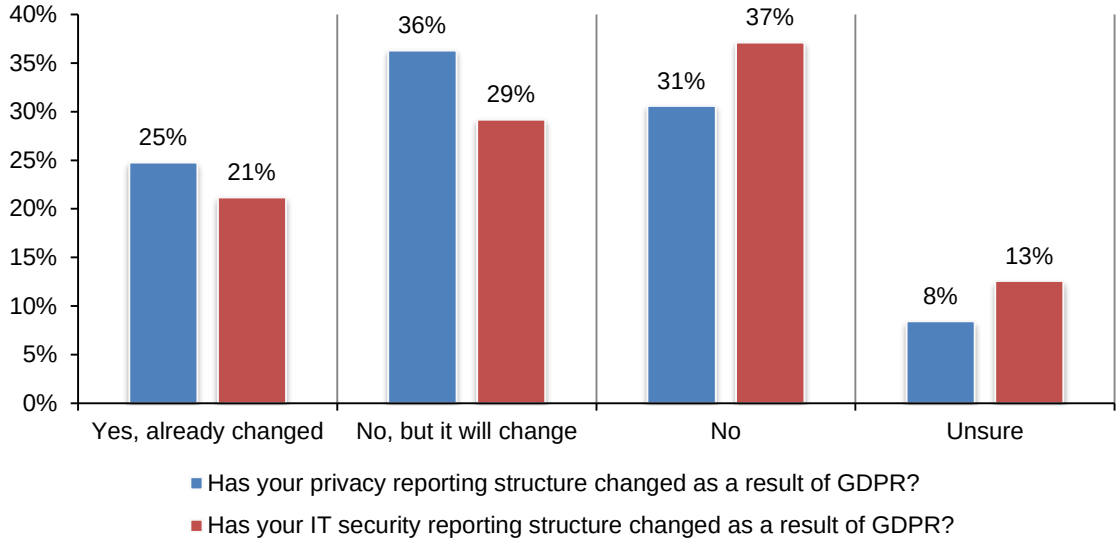
More data protection impact assessments (DPIAs) will be conducted after May 25. As shown in Figure 24, prior to the May 25 deadline 50 percent of respondents say they conducted only one DPIA and 29 percent of respondents say they didn't conduct any. Following the May 25 deadline, 57 percent of respondents say they will conduct at least 3 (44 percent) and more than 5 (13 percent).

FIGURE 24. DPIAS CONDUCTED AND WILL BE CONDUCTED AFTER THE INTRODUCTION OF GDPR



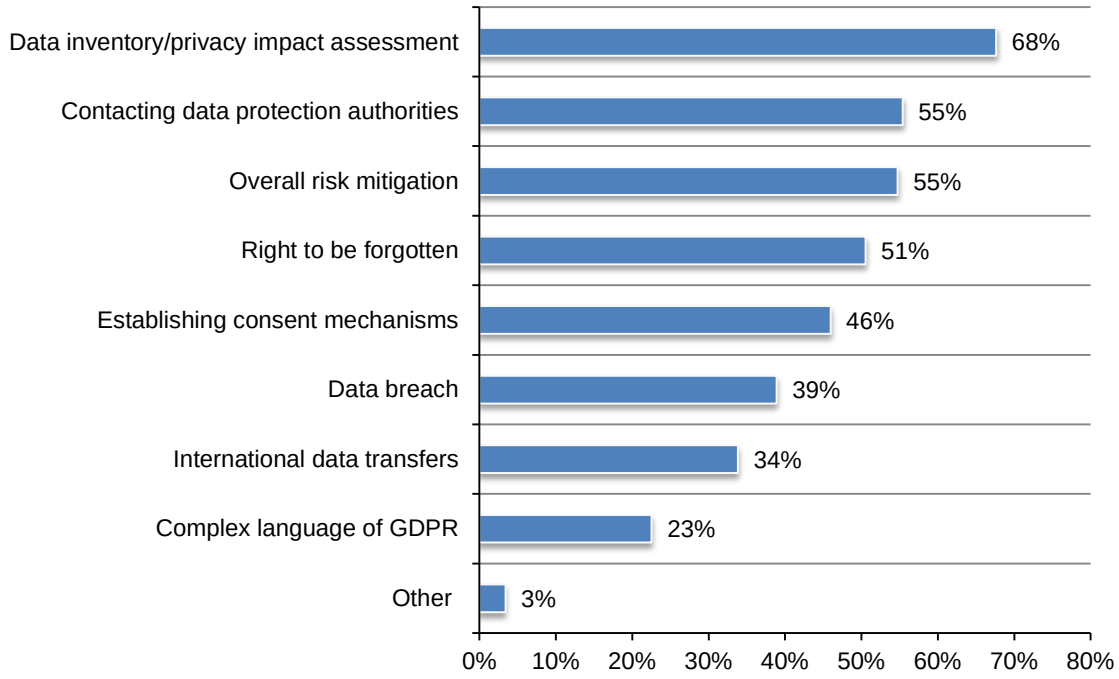
Respondents anticipate changes in their privacy and IT security reporting as a result of GDPR. According to Figure 25, 61 percent of respondents say their privacy reporting structure has already changed or will change as a result of GDPR and 50 percent of respondents say their organizations' IT security reporting structure has changed or will change as a result of GDPR.

FIGURE 25. HAS YOUR PRIVACY AND IT SECURITY REPORTING CHANGED AS A RESULT OF GDPR?



Many companies will hire outside counsel to assist with GDPR compliance. Forty-six percent of respondents say they will hire outside counsel to support their GDPR compliance activities. As shown in Figure 26, the primary reason is to assist with the increasing number of DPIAs that will be conducted (68 percent of respondents). Fifty-five percent of respondents say outside counsel will establish relationships with data protection authorities and another 55 percent of respondents say it will be to assist with overall risk mitigation.

FIGURE 26. WHY WOULD YOU HIRE OUTSIDE COUNSEL TO ASSIST WITH GDPR COMPLIANCE?



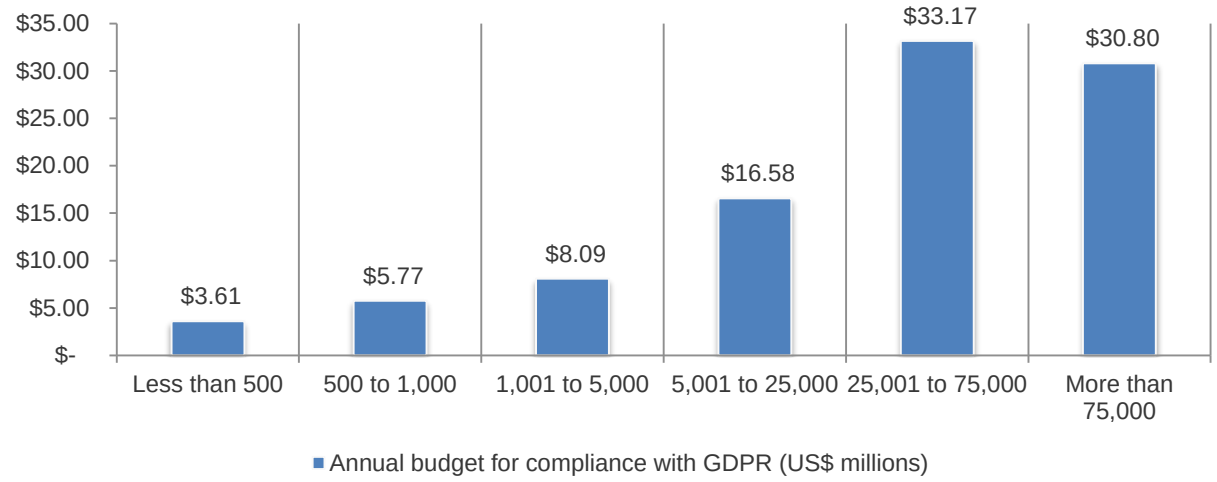
THE GDPR BUDGET

The average annual budget for compliance with GDPR is $13 million. Thirty-three percent of respondents believe the budget for GDPR will be renewed annually and 22 percent of respondents say the budget will continue indefinitely.

As shown in Figure 27, the annual budget for compliance does vary by organizational headcount. The budget for organizations with a headcount of more than 25,000 is significantly higher than those organizations with a smaller headcount. However, because of economies of scale the average per capita budget for organizations with a headcount over 5,000 is $351.59.

FIGURE 27. ANNUAL BUDGET FOR COMPLIANCE WITH GDPR BY ORGANIZATIONAL HEADCOUNT

US$ millions



Most of the budget is allocated to managed services. As shown in Table 1, companies are spending most of their budget on managed services followed by personnel and technologies.

TABLE 1. SEVEN AREAS FOR GDPR BUDGET	TOTAL
Technologies	17%
Personnel	19%
Consultants	10%
Managed services	28%
Outside lawyers	9%
Training	7%
Business process engineering	10%
TOTAL	**100%**

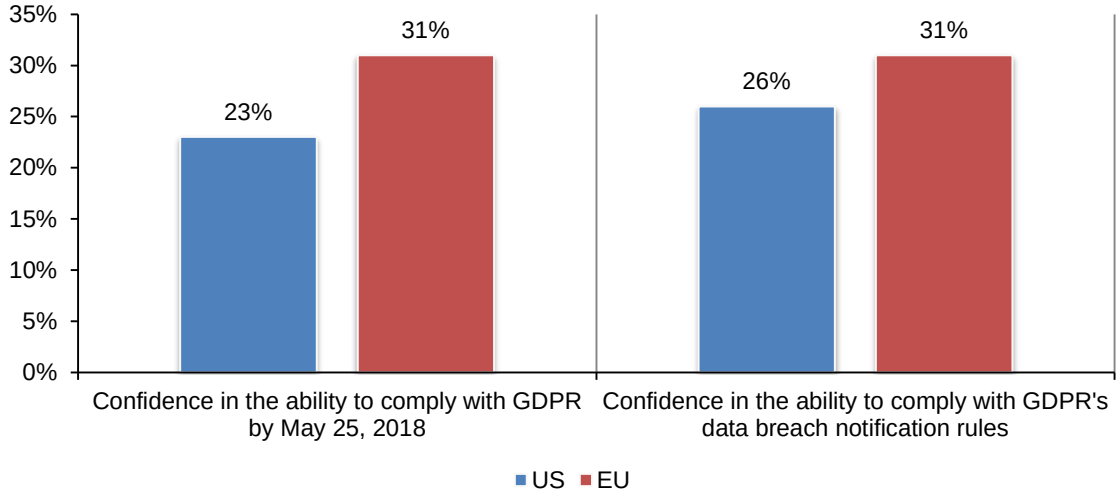
A COMPARISON OF US AND EU RESPONDENTS

In this section we present the other most salient differences between respondents in the US and EU regarding GDPR compliance.

Confidence in meeting the GDPR deadline and data breach notification rules is low in both the US and EU. As shown in Figure 28, only 23 percent of US respondents and 31 percent of EU respondents say they are confident they will meet the GDPR deadline by May 25. Similarly, confidence is low in meeting the data breach notification rules, according to 26 percent of US respondents and 31 percent of EU respondents, respectively.

FIGURE 28. CONFIDENCE IN COMPLYING WITH GDPR

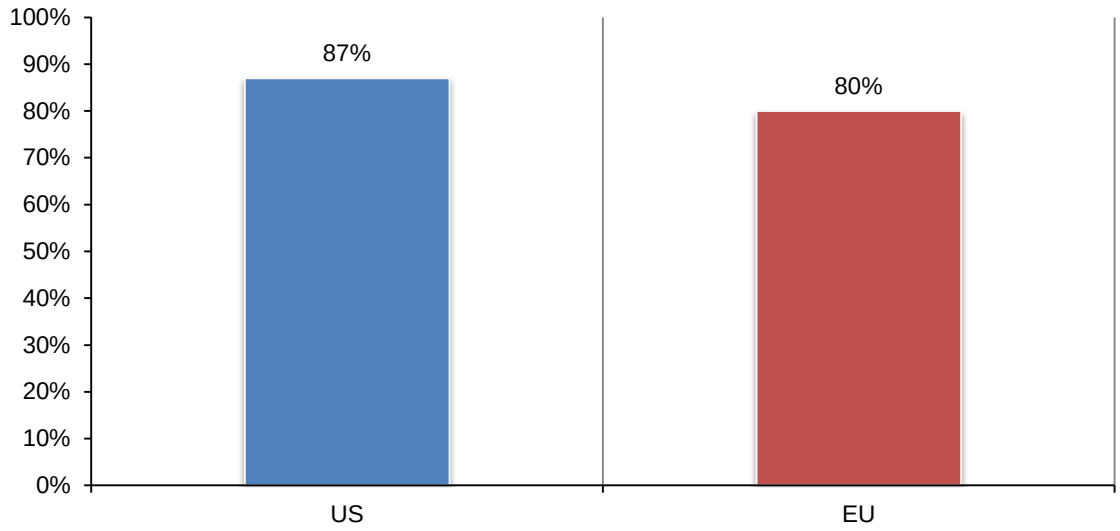
1 = low confidence to 10 = high confidence, 7+ responses combined



Both respondents in the US and EU worry that their profile with regulators increases the risk of fines and penalties. While higher in the US (87 percent of respondents), EU respondents also worry they may be a target for regulatory action, as shown in Figure 29.

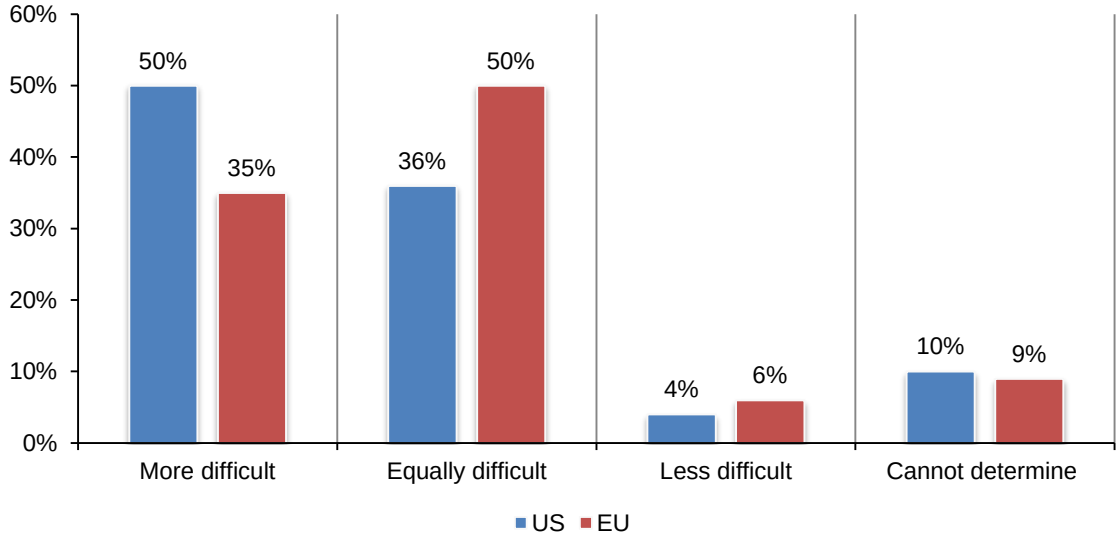
FIGURE 29. THE RISK OF POSSIBLE EU REGULATORY ACTION BECAUSE OF THE ORGANIZATION'S PROFILE WITH REGULATORS

1 = low risk to 10 = high risk, 7+ responses combined



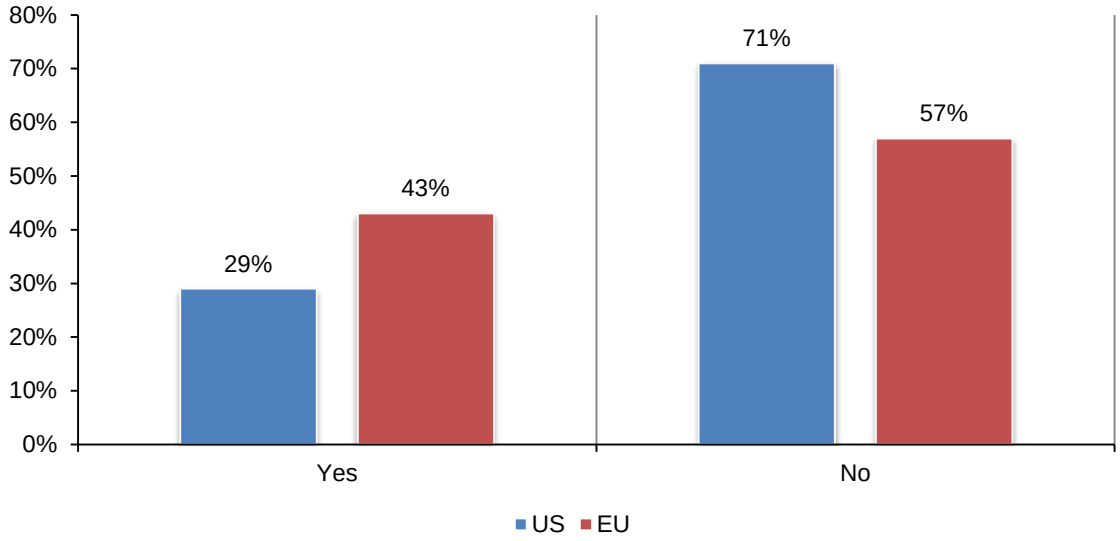
US respondents are likely to say that GDPR is more difficult to comply with than data privacy and security requirements. According to Figure 30, 50 percent of US respondents versus 35 percent of EU respondents say GDPR exceeds other requirements in its level of difficulty.

FIGURE 30. RELATIVE TO OTHER DATA PRIVACY AND SECURITY REQUIREMENTS, HOW DIFFICULT WILL THE GDPR BE TO IMPLEMENT?



More EU organizations have conducted a data inventory or audit of their EU personal information. As shown in Figure 31, only 29 percent of US respondents versus 43 percent of EU respondents say they have conducted a data inventory of their EU personal information to understand how it is used and where it is located.

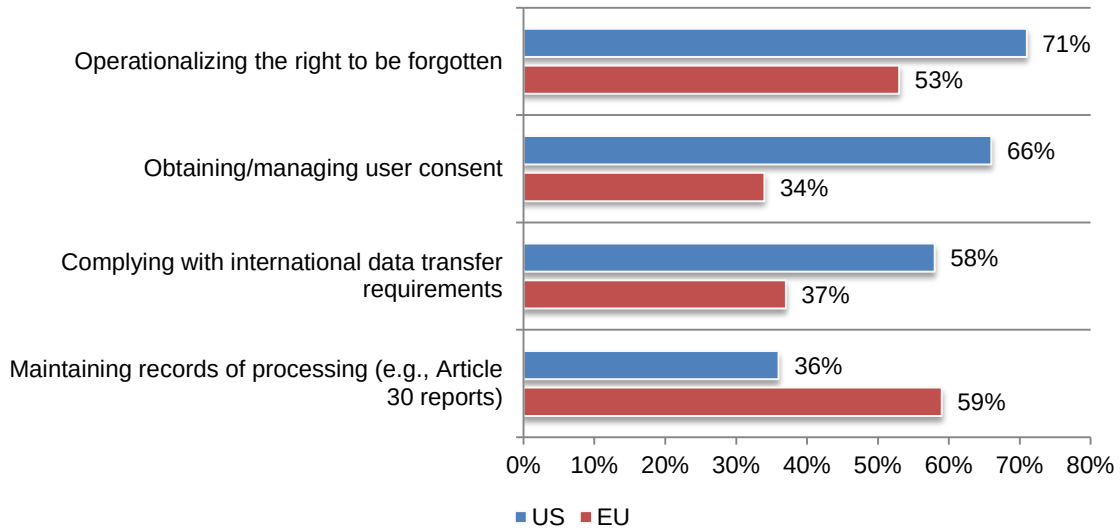
FIGURE 31. HAS YOUR ORGANIZATION CONDUCTED A DATA INVENTORY OR AUDIT OF ITS EU PERSONAL INFORMATION TO UNDERSTAND HOW IT IS USED AND WHERE IT IS LOCATED?



US organizations are more likely to believe they are at risk for non-compliance with GDPR. According to Figure 32, a higher percentage of US respondents believe they are at greater risk for noncompliance if they do not meet the following obligations: operationalizing the right to be forgotten (71 percent of respondents), obtaining/managing user consent (66 percent of respondents) and complying with international data transfer requirements (58 percent of respondents). EU respondents are more concerned than US respondents about the requirement to maintain records of processing (*e.g.*, Article 30 reports).

FIGURE 32. THE RISK OF FAILING TO COMPLY WITH GDPR OBLIGATIONS

7+ on a scale of 1 = low risk to 10 = high risk



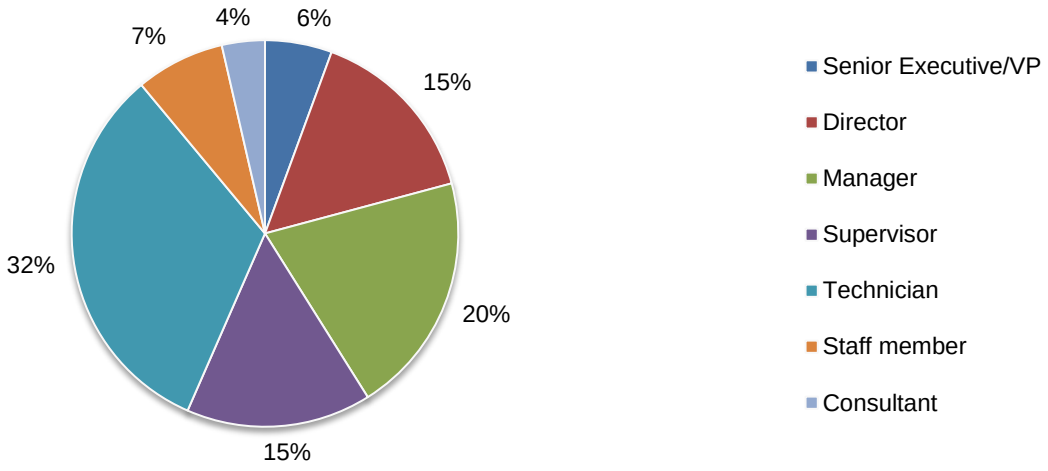
Part 3. Methods and limitations

A sampling frame of 29,674 individuals who work in a variety of departments including information technology (IT), IT security, compliance, legal, data protection office and privacy, were selected as participants in the research. Table 2 shows 1,256 total returns. Screening and reliability checks required the removal of 146 surveys. Our final sample consisted of 1,003 surveys, or a 3.4 percent response rate.

TABLE 2. SAMPLE RESPONSE	US	EU	TOTAL
Total sampling frame	16,783	12,891	29,674
Total survey returns	716	540	1,256
Rejected surveys	84	62	146
Final sample	582	421	1,003
Response rate	3.5%	3.3%	3.4%

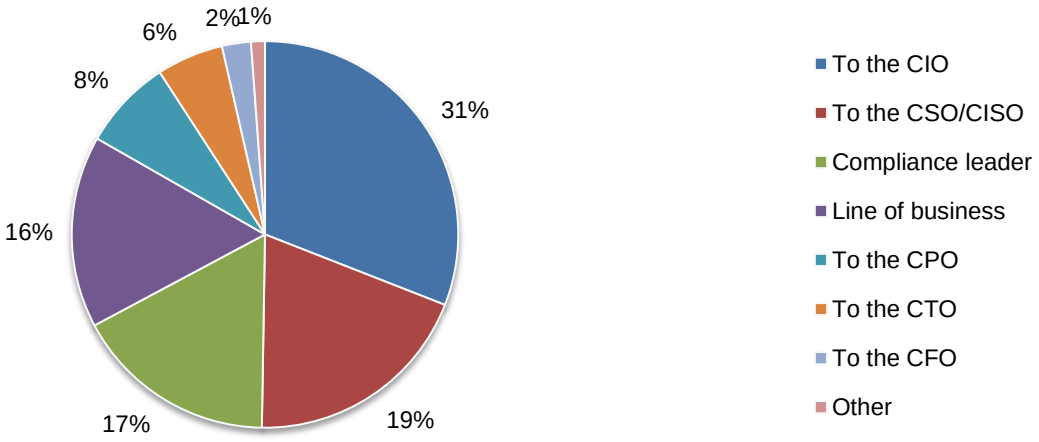
Pie Chart 1 summarizes the approximate position or organizational level of respondents in our study. As can be seen, half of the respondents (51 percent) are at or above the supervisory level.

PIE CHART 1. DISTRIBUTION OF RESPONDENTS ACCORDING TO POSITION OR ORGANIZATIONAL LEVEL



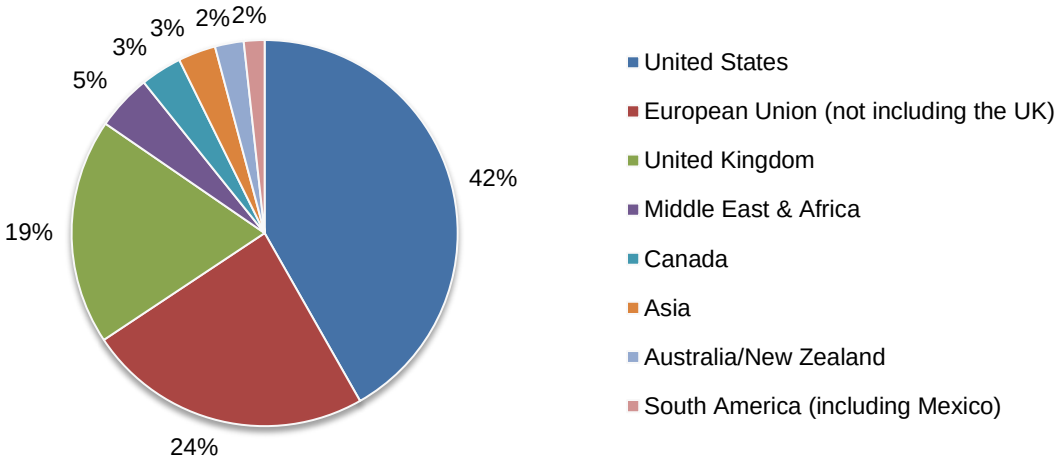
Pie Chart 2 reveals that 31 percent of respondents say their department reports to the CIO, 19 percent report to the CSO/CISO, 17 percent report to the compliance leader and 16 percent report to the lines-of-business leader.

PIE CHART 2. DEPARTMENT REPORTING CHANNEL WITHIN THE ORGANIZATION



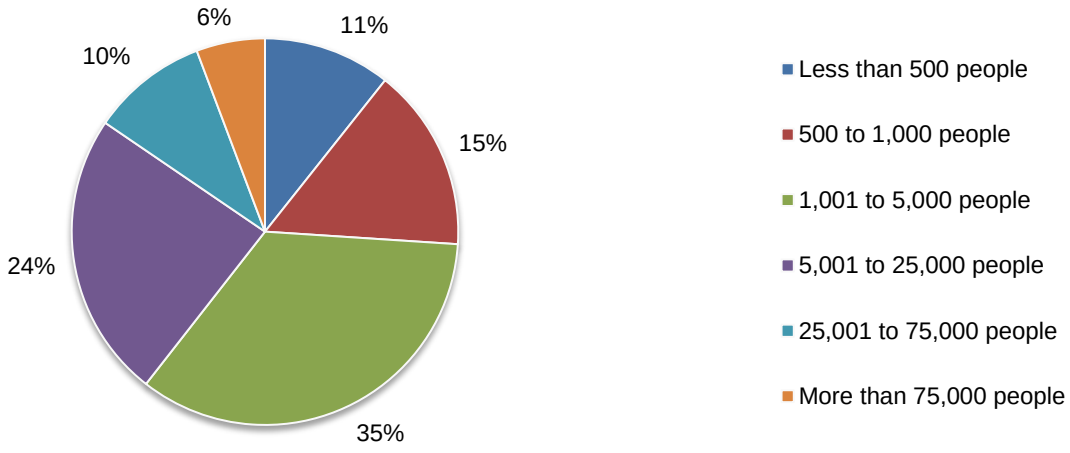
Forty-two percent of respondents indicated their headquarters is located in the US, as shown in Pie Chart 3. Another 24 percent of respondents reported their headquarters is located in the EU (not including the United Kingdom), and 19 percent of respondents reported their headquarters is in the United Kingdom.

PIE CHART 3. LOCATION OF HEADQUARTERS



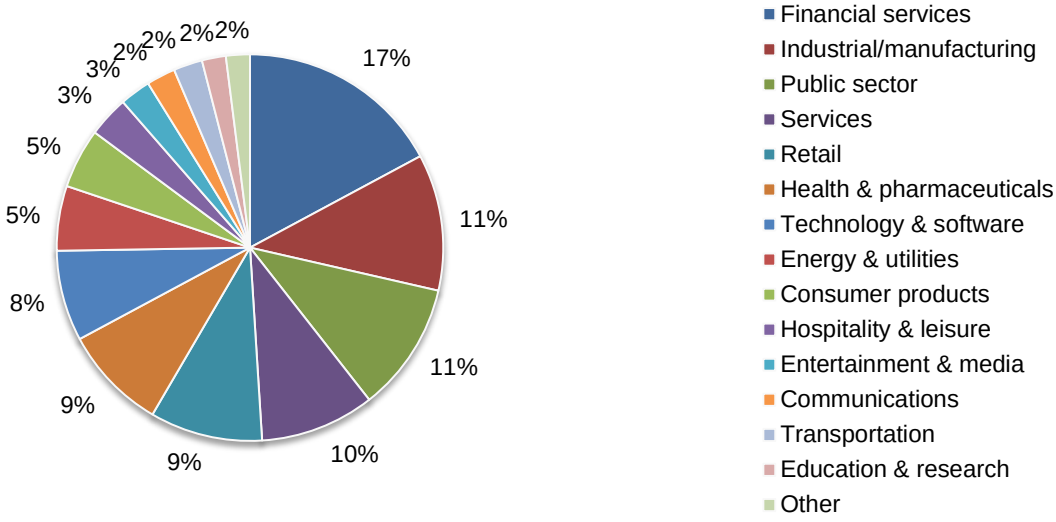
The majority of respondents, 75 percent of the respondents, are from organizations with a global headcount of more than 1,000 employees, as shown in Pie Chart 4.

PIE CHART 4. WORLDWIDE HEADCOUNT OF THE ORGANIZATION



Pie Chart 5 reports the industry classification of respondents' organizations. This chart identifies financial services as the largest segment (17 percent of respondents), followed by industrial/manufacturing (11 percent of respondents), public sector (11 percent of respondents), and service sector (10 percent of respondents).

PIE CHART 5. PRIMARY INDUSTRY CLASSIFICATION



Part 4. Caveats to this study

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most Web-based surveys.

- **Non-response bias:** The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.
- **Sampling-frame bias:** The accuracy is based on contact information and the degree to which the list is representative of individuals involved in IT, IT security, compliance, legal, data protection office and privacy. We also acknowledge that the results may be biased by external events, such as media coverage. Finally, because we used a Web-based collection method, it is possible that non-Web responses made by mailed survey or telephone call would result in a different pattern of findings.
- **Self-reported results:** The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were fielded and collected in February 2018.

SURVEY RESPONSE	TOTAL
Total sampling frame	29,674
Total survey returns	1,256
Rejected surveys	146
Final sample	1,003
Response rate	3.4%
Sample weights	1.00

PART 1. SCREENING QUESTIONS

S1. IS YOUR COMPANY SUBJECT TO GDPR?	TOTAL
Yes	90%
Unsure	10%
No (Stop)	0%
Total	**100%**

S2. HOW FAMILIAR ARE YOU WITH THE GDPR?	TOTAL
Very familiar	35%
Familiar	48%
Not familiar	17%
No knowledge (stop)	0%
Total	**100%**

S3. WILL THE GDPR IMPACT YOUR ORGANIZATION?	TOTAL
Yes, significant impact	35%
Yes, some impact	46%
Yes, nominal impact	20%
No impact (stop)	0%
Total	**100%**

PART 2. BACKGROUND

Q1. IN WHICH DEPARTMENT DO YOU WORK?	TOTAL
Privacy	11%
Data Protection Office	14%
Compliance	18%
Legal	20%
IT	22%
IT security	15%
None of the above	0%
Total	**100%**

Q2. DO YOU OFFER GOODS OR SERVICES TO DATA SUBJECTS IN THE EU, FOR SALE OR FREE?	TOTAL
Yes	97%
No	3%
Total	**100%**

Q3. DO YOU TRACK OR OBSERVE THE BEHAVIOR OF EU RESIDENTS IN THE EU BY USING COOKIES OR OTHER METHODS?	TOTAL
Yes	56%
No	44%
Total	**100%**

Q4. TO TRANSMIT EU PERSONAL DATA OUTSIDE OF THE EU, WHAT MECHANISMS DOES YOUR COMPANY USE OR INTEND TO USE? PLEASE CHECK ALL THAT APPLY.	TOTAL
Standard Contractual Clauses	83%
Consent	67%
Other statutory derogations, such as fulfillment of contract	41%
Certification or seal framework to be determined under GDPR	29%
Adequacy	43%
Binding Corporate Rules (BCR)	19%
Privacy Shield	25%
None of the above	9%
Total	**316%**

Q5A. DO YOU EXPECT TO CHANGE ANY DATA TRANSFER MECHANISMS?	TOTAL
Yes	46%
No	46%
Unsure	8%
Total	**100%**

Q5B. IF SO, WHICH MECHANISMS WILL YOUR ORGANIZATION CHANGE TO?	TOTAL
Standard Contractual Clauses	36%
Consent	30%
Other statutory derogations, such as fulfillment of contract	14%
Certification or seal framework to be determined under GDPR	48%
Adequacy	26%
Binding Corporate Rules (BCR)	29%
Privacy Shield	37%
None of the above	14%
Total	**234%**

Q6A. WHAT DO YOU CONSIDER YOUR ORGANIZATION TO BE?	TOTAL
Controller	39%
Processor	30%
Both processor and controller	30%
Total	**100%**

Q6B. IF YOU ARE A PROCESSOR, ARE YOU CONTEMPLATING BECOMING A CONTROLLER BECAUSE OF GDPR?	TOTAL
Yes	37%
No	55%
Unsure	7%
Total	**100%**

Q7. DOES YOUR ORGANIZATION CONDUCT THE FOLLOWING PRACTICES WITH YOUR OFFICES AND THIRD PARTIES THROUGHOUT THE WORLD? PLEASE CHECK ALL THAT APPLY.	TOTAL
Marketing and customer outreach	83%
Advertising and promotion campaigns	87%
Call centers and customer service operations	91%
Data processing operations including the use of cloud infrastructure	74%
Research and development	64%
Sales management	87%
Payment transaction processing	72%
Data hygiene and quality control	62%
Identity, authentication and security management	64%
Application development and testing	53%
Other (please specify)	3%
Total	**741%**

Q8A. HAS YOUR ORGANIZATION EVER EXPERIENCED A DATA BREACH INVOLVING PERSONAL DATA OF EU INDIVIDUALS CAUSED BY EMPLOYEE NEGLIGENCE, SYSTEM GLITCH AND/OR THIRD-PARTY MISTAKES INVOLVING THE LOSS OF SENSITIVE PERSONAL INFORMATION?	TOTAL
Yes	42%
No	47%
Unsure	11%
Total	**100%**

Q8B. HAS YOUR ORGANIZATION EVER EXPERIENCED A DATA BREACH INVOLVING PERSONAL DATA OF EU INDIVIDUALS CAUSED BY A CRIMINAL ATTACK INVOLVING THE LOSS OF SENSITIVE PERSONAL INFORMATION?	TOTAL
Yes	33%
No	56%
Unsure	12%
Total	**100%**

Q8C. IF YES, WHAT WERE THE ROOT CAUSES OF THESE DATA BREACHES? PLEASE SELECT ALL THAT APPLY.	TOTAL
Negligent insider	33%
Malicious insider	14%
Systems glitch	15%
Cyber attack	33%
Outsourcing data to a third party	16%
Data lost in physical delivery	12%
Failure to protect actual documents	44%
Other (please specify)	4%
Do not know	10%
Total	**181%**

Q9A. DOES YOUR ORGANIZATION HAVE A DATA GOVERNANCE PROGRAM?	TOTAL
Yes, a formal program	31%
Yes, an informal or “ad hoc” program	26%
No	43%
Total	**100%**

Q9B. IF YES, WHAT BEST DESCRIBES THE MATURITY LEVEL OF YOUR ORGANIZATION’S DATA GOVERNANCE PROGRAM?	TOTAL
Early stage – many data governance program activities have not as yet been planned or deployed	29%
Middle stage – data governance program activities are planned and defined but only partially deployed	35%
Late-middle stage – many data governance program activities are deployed across the enterprise	21%
Mature stage – Core data governance program activities are deployed, maintained and/or refined across the enterprise	15%
Total	**100%**

PART 3. ATTRIBUTIONS AND IMPORTANCE OF GDPR

PLEASE RATE EACH STATEMENT ABOUT GDPR USING THE SCALE PROVIDED BELOW EACH ITEM TO EXPRESS YOUR OPINION. STRONGLY AGREE AND AGREE RESPONSES COMBINED.	TOTAL
Q10a. Compliance with GDPR is a strategic priority for our organization.	57%
Q10b. Failure to comply with GDPR would have a detrimental impact on our organization's ability to conduct business globally.	71%
Q10c. Our senior leaders and board of directors are fully aware of our organization's state of compliance with GDPR.	37%
Q10d. Senior leadership is concerned that failure to comply with GDPR might affect them personally.	46%
Q10e. Our organization would consider changing its operations in Europe because of overly strict compliance requirements.	21%
Q10f. GDPR will significantly change my organization's workflows regarding the collection, use and protection of personal information.	60%

PART 4. COMPLIANCE WITH THE GDPR AND PERCEPTION OF RISK

Q11. USING THE FOLLOWING 10-POINT SCALE, PLEASE RATE YOUR ORGANIZATION'S LEVEL OF READINESS TO COMPLY WITH THE GDPR. 1 = NOT READY TO 10 = HIGH READINESS.	TOTAL
1 or 2	10%
3 or 4	21%
5 or 6	35%
7 or 8	19%
9 or 10	15%
Total	**100%**
Extrapolated value	**5.66**

Q12. USING THE FOLLOWING 10-POINT SCALE, PLEASE RATE YOUR ORGANIZATION'S LEVEL OF RISK OF POSSIBLE EU REGULATORY ACTION BECAUSE OF ITS PROFILE WITH REGULATORS. 1 = LOW RISK TO 10 = HIGH RISK.	TOTAL
1 or 2	0%
3 or 4	4%
5 or 6	11%
7 or 8	39%
9 or 10	45%
Total	**100%**
Extrapolated value	**7.98**

Q13. RELATIVE TO OTHER DATA PRIVACY AND SECURITY REQUIREMENTS, HOW DIFFICULT WILL THE GDPR BE TO IMPLEMENT?	TOTAL
More difficult	44%
Equally difficult	42%
Less difficult	5%
Cannot determine	10%
Total	**100%**

Q14A. DOES YOUR ORGANIZATION UNDERSTAND WHAT IT NEEDS TO DO TO COMPLY WITH THE GDPR?	TOTAL
Yes	53%
No	47%
Total	**100%**

Q14B. IF YES, HOW IS YOUR COMPANY PREPARING FOR COMPLIANCE WITH GDPR? PLEASE CHECK ALL THAT APPLY.	TOTAL
Appointing a data protection officer under the GDPR	92%
Allocating budget specifically for compliance with the GDPR	57%
Informing senior leadership and the board of directors about the Regulation's requirements	53%
Conducting an assessment of our ability to comply with the regulations	62%
Investing in new technologies or services (i.e., analytics and reporting, consent management, encryption) to prepare for the new requirements	41%
Creating a new reporting structure	20%
Creating a new accountability framework	15%
Putting in place a new data transfer mechanism	21%
Changing or closing our overseas operations	20%
Evaluating and adjusting relationships with our third-party vendors	33%
Adding staff	36%
Other (please specify)	4%
None of the above	2%
Total	**455%**

Q15A. USING THE FOLLOWING 10-POINT SCALE, PLEASE RATE YOUR ORGANIZATION'S LEVEL OF READINESS TO RESPOND TO A DATA BREACH INVOLVING PERSONAL DATA OF EU INDIVIDUALS. 1 = LOW READINESS AND 10 = HIGH READINESS	TOTAL
1 or 2	7%
3 or 4	16%
5 or 6	42%
7 or 8	20%
9 or 10	15%
Total	**100%**
Extrapolated value	**5.87**

Q15B. WHAT CONSEQUENCES OF A POTENTIAL DATA BREACH INVOLVING PERSONAL DATA OF EU INDIVIDUALS ARE YOU MOST CONCERNED ABOUT? PLEASE SELECT YOUR TOP THREE CONCERNS.	TOTAL
Caused significant brand and reputation damage	22%
C-level executive was forced to resign	10%
Caused significant financial harm	46%
Made our organization more vulnerable to future breach and other security incidents	40%
Decreased customer and consumer trust in our organization	23%
Negative media coverage	12%
Decline in company's share price	33%
Loss of productivity	35%
Legal action	25%
Regulatory fines	53%
Other	1%
Total	**300%**

Q16. USING THE FOLLOWING 10-POINT SCALE, PLEASE RATE YOUR ORGANIZATION'S CONFIDENCE TO COMPLY WITH THE GDPR BY MAY 25, 2018. 1 = LOW CONFIDENCE AND 10 = HIGH CONFIDENCE	TOTAL
1 or 2	9%
3 or 4	29%
5 or 6	35%
7 or 8	19%
9 or 10	7%
Total	**100%**
Extrapolated value	**5.21**

Q17A. USING THE FOLLOWING 10-POINT SCALE, PLEASE RATE YOUR ORGANIZATION'S CONFIDENCE TO COMPLY WITH THE GDPR'S DATA BREACH NOTIFICATION RULES. 1 = LOW CONFIDENCE AND 10 = HIGH CONFIDENCE	TOTAL
1 or 2	12%
3 or 4	20%
5 or 6	40%
7 or 8	20%
9 or 10	8%
Total	**100%**
Extrapolated value	**5.34**

Q17B. IF YOU RATED YOUR CONFIDENCE 7 OR HIGHER TO COMPLY WITH THE GDPR'S DATA BREACH NOTIFICATION RULES, WHY ARE YOU CONFIDENT?	TOTAL
Our organization has the necessary security technologies in place to be able to detect the occurrence of a data breach quickly	56%
Our organization's incident response plan has proven to be effective in providing timely notification	66%
Our organization is able to provide notification to the data protection authority within 72 hours	14%
Our organization would be able to determine quickly if the breach is unlikely to result in a "risk for the rights and freedoms of natural persons"	24%
Other (please specify)	3%
None of the above	23%
Total	**184%**

Q18. WHEN DO YOU EXPECT YOUR ORGANIZATION WILL BE SATISFIED WITH ITS EFFORTS TO BE IN COMPLIANCE WITH GDPR?	TOTAL
Before May 25, 2018	10%
At May 25, 2018	42%
After May 25, 2018	40%
Don't know	8%
Total	**100%**

Q19. AFTER BECOMING COMPLIANT, WHAT DO YOU EXPECT YOUR ORGANIZATION'S WORKLOAD TO BE IN ORDER TO MAINTAIN GDPR COMPLIANCE?	TOTAL
Workload will increase	44%
Workload will stay the same	41%
Workload will decrease	15%
Total	**100%**

Q20. WHICH OF THE FOLLOWING WILL REQUIRE SIGNIFICANT EFFORTS AFTER MAY 25? PLEASE CHECK ALL THAT APPLY.	TOTAL
A data protection officer under the GDPR	2%
A budget specifically for compliance with the GDPR	10%
Ongoing updates to senior leadership and the board of directors about the Regulation's requirements	18%
Assessments of our ability to comply with the regulations	65%
Investments in new technologies or services (*i.e.*, analytics and reporting, consent management, encryption) to maintain compliance	72%
Creation of a new reporting structure	46%
Creation of a new accountability framework	52%
Put in place a new data transfer mechanism	35%
Change or close our operations in Europe	9%
Evaluate relationships with our third-party vendors	58%
Total	**367%**

Q21. HAS YOUR ORGANIZATION CONDUCTED A DATA INVENTORY OR AUDIT OF ITS EU PERSONAL INFORMATION TO UNDERSTAND HOW INFORMATION IS USED AND WHERE IT IS LOCATED?	TOTAL
Yes	35%
No	65%
Total	**100%**

Q22A. HOW MANY DATA PROTECTION IMPACT ASSESSMENTS (DPIA) OF YOUR ORGANIZATION'S EU PERSONAL INFORMATION, AS OUTLINED IN THE GDPR, HAVE BEEN CONDUCTED TO UNDERSTAND HOW INFORMATION IS USED AND WHERE IT IS LOCATED?	TOTAL
None	29%
1 or 2	50%
3 to 5	15%
More than 5	6%
Total	**100%**

Q22B. HOW MANY DATA PROTECTION IMPACT ASSESSMENTS (DPIA) DO YOU ANTICIPATE HAVING TO DO AFTER THE INTRODUCTION OF GDPR?	TOTAL
None	9%
1 or 2	34%
3 to 5	44%
More than 5	13%
Total	**100%**

Q23. WHAT ARE THE BARRIERS TO GDPR COMPLIANCE? PLEASE SELECT THE TOP THREE BARRIERS.	TOTAL
The lack of privacy or security experts knowledgeable about GDPR	22%
The lack of experts knowledgeable about how to respond to a breach involving EU personal data	30%
Insufficient budget to invest in additional staffing	36%
Insufficient budget to invest in appropriate security technologies	36%
The need to make comprehensive changes in business practices	64%
Unrealistic demands from the regulation/regulator	54%
Too little time	55%
Other (please specify)	3%
None of the above	0%
Total	**300%**

Q24. WHAT ARE YOUR TOP CONCERNS ABOUT NON-COMPLIANCE WITH GDPR? PLEASE SELECT THE TOP THREE CONCERNS	TOTAL
New penalties of up to 10 to 20 million euros or 2 to 4 percent of annual worldwide revenue, whichever is greater	72%
Managing cultural expectations when communicating with customers outside of the U.S.	22%
Increased territorial scope, impacting more businesses including many outside the EU	20%
Tighter requirements for obtaining valid consent to the processing of personal data	23%
New restrictions on profiling and targeted advertising	26%
New data breach reporting obligations	43%
Direct legal compliance obligations for “data processors”	27%
Extended data protection rights for individuals, including the “right to be forgotten”	40%
Customer loss	15%
No concern	13%
Total	**300%**

Q25. WHICH OF THE FOLLOWING SECURITY ACTIONS IN GDPR IS YOUR ORGANIZATION PREPARED TO ADDRESS? PLEASE CHECK ALL THAT APPLY.	TOTAL
The pseudonymisation and encryption of personal data	64%
The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services	50%
The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	70%
A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing	52%
Auditing and review of third-party contracts	49%
None of the above	11%
Total	**295**%

Q26. USING THE FOLLOWING 10-POINT SCALE, PLEASE RATE THE RISK OF POTENTIAL REGULATORY ACTION IF YOUR ORGANIZATION FAILS TO COMPLY WITH THE FOLLOWING GDPR OBLIGATIONS. 1 = LOW RISK TO 10 = HIGH RISK

Q26A. OPERATIONALIZING THE RIGHT TO BE FORGOTTEN	TOTAL
1 or 2	9%
3 or 4	10%
5 or 6	18%
7 or 8	28%
9 or 10	36%
Total	**100%**
Extrapolated value	**6.93**

Q26B. OPERATIONALIZING DATA PORTABILITY	TOTAL
1 or 2	13%
3 or 4	19%
5 or 6	23%
7 or 8	29%
9 or 10	16%
Total	**100%**
Extrapolated value	**5.81**

Q26C. OBTAINING/MANAGING USER CONSENT	TOTAL
1 or 2	7%
3 or 4	15%
5 or 6	25%
7 or 8	23%
9 or 10	29%
Total	**100%**
Extrapolated value	**6.55**

Q26D. COMPLYING WITH INTERNATIONAL DATA TRANSFER REQUIREMENTS	TOTAL
1 or 2	12%
3 or 4	15%
5 or 6	24%
7 or 8	22%
9 or 10	27%
Total	**100%**
Extrapolated value	**6.27**

Q26E. PREPARING FOR DATA BREACH NOTIFICATION	TOTAL
1 or 2	4%
3 or 4	14%
5 or 6	15%
7 or 8	29%
9 or 10	39%
Total	**100%**
Extrapolated value	**7.19**

Q26F. CONDUCTING DATA PROTECTION IMPACT ASSESSMENTS	TOTAL
1 or 2	13%
3 or 4	23%
5 or 6	27%
7 or 8	22%
9 or 10	16%
Total	**100%**
Extrapolated value	**5.58**

Q26G. ESTABLISHING LEGITIMATE INTEREST FOR DATA PROCESSING	TOTAL
1 or 2	13%
3 or 4	10%
5 or 6	25%
7 or 8	24%
9 or 10	27%
Total	**100%**
Extrapolated value	**6.31**

Q26H. CONDUCTING DATA INVENTORY/MAPPING	TOTAL
1 or 2	10%
3 or 4	10%
5 or 6	17%
7 or 8	36%
9 or 10	27%
Total	**100%**
Extrapolated value	**6.69**

Q26I. MAINTAINING RECORDS OF PROCESSING (E.G. ARTICLE 30 REPORTS)	TOTAL
1 or 2	13%
3 or 4	15%
5 or 6	27%
7 or 8	29%
9 or 10	16%
Total	**100%**
Extrapolated value	**5.92**

Q26J. MANAGING DATA SUBJECT REQUESTS	TOTAL
1 or 2	14%
3 or 4	15%
5 or 6	25%
7 or 8	27%
9 or 10	19%
Total	**100%**
Extrapolated value	**5.93**

Q26K. APPOINTING A DATA PROTECTION OFFICER (DPO)	TOTAL
1 or 2	20%
3 or 4	26%
5 or 6	29%
7 or 8	19%
9 or 10	5%
Total	**100%**
Extrapolated value	**4.76**

Q27. USING THE FOLLOWING 10-POINT SCALE, PLEASE RATE THE DIFFICULTY IN COMPLYING WITH THE FOLLOWING GDPR OBLIGATIONS. 1 = LOW DIFFICULTY TO 10 = HIGH DIFFICULTY

Q27A. OPERATIONALIZING THE RIGHT TO BE FORGOTTEN	TOTAL
1 or 2	2%
3 or 4	4%
5 or 6	12%
7 or 8	32%
9 or 10	50%
Total	**100%**
Extrapolated value	**7.97**

Q27B. OPERATIONALIZING DATA PORTABILITY	TOTAL
1 or 2	3%
3 or 4	5%
5 or 6	9%
7 or 8	37%
9 or 10	46%
Total	**100%**
Extrapolated value	**7.85**

Q27C. OBTAINING/MANAGING USER CONSENT	TOTAL
1 or 2	6%
3 or 4	12%
5 or 6	19%
7 or 8	28%
9 or 10	36%
Total	**100%**
Extrapolated value	**7.00**

Q27D. COMPLYING WITH INTERNATIONAL DATA TRANSFER REQUIREMENTS	TOTAL
1 or 2	5%
3 or 4	11%
5 or 6	24%
7 or 8	22%
9 or 10	38%
Total	**100%**
Extrapolated value	**7.03**

Q27E. PREPARING FOR DATA BREACH NOTIFICATION	TOTAL
1 or 2	4%
3 or 4	4%
5 or 6	8%
7 or 8	32%
9 or 10	51%
Total	**100%**
Extrapolated value	**7.95**

Q27F. CONDUCTING DATA PROTECTION IMPACT ASSESSMENTS	TOTAL
1 or 2	17%
3 or 4	21%
5 or 6	25%
7 or 8	22%
9 or 10	15%
Total	**100%**
Extrapolated value	**5.45**

Q27G. ESTABLISHING LEGITIMATE INTEREST FOR DATA PROCESSING	TOTAL
1 or 2	22%
3 or 4	26%
5 or 6	28%
7 or 8	17%
9 or 10	7%
Total	**100%**
Extrapolated value	**4.74**

Q27H. CONDUCTING DATA INVENTORY/MAPPING	TOTAL
1 or 2	3%
3 or 4	4%
5 or 6	16%
7 or 8	41%
9 or 10	35%
Total	**100%**
Extrapolated value	**7.52**

Q27I. MAINTAINING RECORDS OF PROCESSING (E.G., ARTICLE 30 REPORTS)	TOTAL
1 or 2	27%
3 or 4	30%
5 or 6	20%
7 or 8	15%
9 or 10	8%
Total	**100%**
Extrapolated value	**4.48**

Q27J. MANAGING DATA SUBJECT REQUESTS	TOTAL
1 or 2	4%
3 or 4	15%
5 or 6	24%
7 or 8	26%
9 or 10	31%
Total	**100%**
Extrapolated value	**6.83**

Q27K. APPOINTING A DATA PROTECTION OFFICER (DPO)	TOTAL
1 or 2	32%
3 or 4	43%
5 or 6	17%
7 or 8	6%
9 or 10	2%
Total	**100%**
Extrapolated value	**3.59**

PART 5. REPORTING STRUCTURE AND HIRING

Q28. HAS YOUR PRIVACY REPORTING STRUCTURE CHANGED AS A RESULT OF GDPR?	TOTAL
Yes, already changed	25%
No, but it will change	36%
No	31%
Unsure	8%
Total	**100%**

Q29. HAS YOUR IT SECURITY REPORTING STRUCTURE CHANGED AS A RESULT OF GDPR?	TOTAL
Yes, already changed	21%
No, but will change	29%
No	37%
Unsure	13%
Total	**100%**

Q30A. TO ASSIST WITH EFFORTS TO COMPLY WITH GDPR HAS YOUR ORGANIZATION HIRED OR WILL HIRE OUTSIDE COUNSEL?	TOTAL
Yes	46%
No	49%
Unsure	5%
Total	**100%**

Q30B. IF YES, WHY WOULD YOU HIRE OUTSIDE COUNSEL TO ASSIST WITH GDPR COMPLIANCE? PLEASE CHECK ALL THAT APPLY.	TOTAL
Complex language of GDPR	23%
Overall risk mitigation	55%
International data transfers	34%
Data breach	39%
Right to be forgotten	51%
Establishing consent mechanisms	46%
Data inventory/privacy impact assessment	68%
Contacting data protection authorities	55%
Other (please specify)	3%
Total	**373%**

Q31. DO YOU PLAN ON HIRING MORE EMPLOYEES AFTER MAY 25, 2018 TO PROVIDE ONGOING ASSISTANCE WITH GDPR?	TOTAL
Yes	48%
No	45%
Unsure	7%
Total	**100%**

PART 6. BUDGET

Q32A. HAS YOUR ORGANIZATION ALLOCATED BUDGET SPECIFICALLY FOR COMPLIANCE WITH THE GDPR?	TOTAL
Yes	61%
No (skip to Part 7)	39%
Total	**100%**

Q32B. IF YES, DID YOUR ORGANIZATION ALLOCATE FUNDING FOR GDPR COMPLIANCE BECAUSE OF A DATA BREACH OR CYBER EXPLOIT?	TOTAL
Yes	44%
No	56%
Total	**100%**

Q33. APPROXIMATELY, WHAT IS THE DOLLAR RANGE THAT BEST DESCRIBES YOUR ORGANIZATION'S ANNUAL BUDGET FOR COMPLIANCE WITH GDPR?	TOTAL
Less than $500,000	1%
$500,001 to $1 million	7%
$1 to $5 million	14%
$6 to $10 million	25%
$11 to $15 million	23%
$16 to $20 million	16%
$21 to $25 million	9%
$26 to $50 million	4%
More than $50 million	2%
Total	**100%**
Extrapolated value (US$ millions)	**$13.04**

**Euro converted into US dollars*

Q34. DO YOU BELIEVE THIS IS A ONE-TIME BUDGET ALLOCATED TO GDPR COMPLIANCE?	TOTAL
Yes, one-time allocation	38%
No, the budget will be renewed annually	33%
No, the budget will continue indefinitely	22%
Unsure	7%
Total	**100%**

Q35. THE FOLLOWING TABLE LISTS SEVEN AREAS OF A GDPR BUDGET. PLEASE ALLOCATE 100 POINTS TO DENOTE THE LEVEL OF INVESTMENT IN EACH AREA.

SEVEN AREAS FOR GDPR BUDGET	TOTAL
Technologies	17
Personnel	18
Consultants	10
Managed services	28
Outside lawyers	9
Training	7
Business process engineering	10
Total=100 points	**100**

Q36. WHO CONTROLS THE GDPR BUDGET? PLEASE CHECK ALL THAT APPLY.	TOTAL
CEO/COO	1%
Chief compliance officer (CCO)	7%
General counsel (OGC)	4%
General manager / VP lines of business	21%
Chief risk officer (CRO)	7%
Chief information officer (CIO)	43%
Chief information security officer (CISO/CSO)	17%
Chief technology officer (CTO)	5%
Data protection officer (DPO)	17%
Chief privacy officer (CPO)	11%
No one person is responsible	35%
Other (please specify)	3%
Total	**171%**

Q37. DOES YOUR ORGANIZATION EARMARK FUNDING FOR BINDING CORPORATE RULES (BCR)?	TOTAL
Yes	33%
No	67%
Total	**100%**

Q38. DOES YOUR ORGANIZATION EARMARK FUNDING FOR PRIVACY SHIELD?	TOTAL
Yes	23%
No	77%
Total	**100%**

D1. WHAT ORGANIZATIONAL LEVEL BEST DESCRIBES YOUR CURRENT POSITION?	TOTAL
Senior Executive/VP	6%
Director	15%
Manager	20%
Supervisor	15%
Technician	32%
Staff member	7%
Consultant	4%
Other (please specify)	0%
Total	**100%**

D2. WHERE DOES YOUR DEPARTMENT REPORT IN THE ORGANIZATION?	TOTAL
To the CFO	2%
To the CTO	6%
To the CIO	31%
To the CSO/CISO	19%
To the CPO	8%
Compliance leader	17%
Line of business (LOB)	16%
Other (please specify)	1%
Total	**100%**

D3. WHERE IS YOUR ORGANIZATION HEADQUARTERED?	TOTAL
United States	42%
European Union (not including the United Kingdom)	23%
United Kingdom	19%
Canada	3%
Asia	3%
South America (including Mexico)	2%
Middle East & Africa	5%
Australia/New Zealand	2%
Total	**100%**

D4. WHAT IS THE WORLDWIDE HEADCOUNT OF YOUR ORGANIZATION?	TOTAL
Less than 500 people	11%
500 to 1,000 people	15%
1,001 to 5,000 people	35%
5,001 to 25,000 people	24%
25,001 to 75,000 people	10%
More than 75,000 people	6%
Total	**100%**

D5. WHAT INDUSTRY BEST DESCRIBES YOUR ORGANIZATION'S INDUSTRY FOCUS?	TOTAL
Agriculture & food services	1%
Communications	2%
Consumer products	5%
Defense & aerospace	1%
Education & research	2%
Energy & utilities	5%
Entertainment & media	3%
Financial services	17%
Health & pharmaceuticals	9%
Hospitality & leisure	3%
Industrial/manufacturing	11%
Public sector	11%
Retail	9%
Services	10%
Technology & software	8%
Transportation	2%
Other (please specify)	0%
Total	**100%**

PONEMON INSTITUTE

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

We uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict confidentiality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.

Please contact research@ponemon.org or call us at +1 800 887 3118 if you have any questions.

ABOUT McDERMOTT

McDermott Will & Emery is a leading international firm with a diversified business practice. Currently numbering more than 1,000 lawyers, we have 19 offices worldwide and a strategic alliance with MWE China Law Offices in Shanghai.

McDermott's world-class Global Privacy and Cybersecurity team includes more than 50 privacy and cybersecurity lawyers advising clients on the statutory, regulatory and enforcement regimes that govern the collection, use and disclosure of data in the United States, Europe, Asia and elsewhere. We have extensive experience advising on the full range of data privacy and protection laws, industry standards and issues. Our lawyers regularly counsel clients on US and international data-use issues, data transfers, and privacy compliance under US and foreign laws. We conduct in-depth privacy/cybersecurity risk assessments, often in the context of mergers, acquisitions and other domestic and cross-border transactions.

Questions regarding our Global Privacy and Cybersecurity work, please contact:

Mark E. Schreiber | Boston | mschreiber@mwe.com | +1 617 535 3982
Ashley Winton | London | awinton@mwe.com | +44 20 7577 6939

For more information regarding McDermott's Global Privacy and Cybersecurity capabilities, visit **www.mwe.com/gdpr.**