

RESEARCH REPORT



# Privacy and the EU GDPR

## US and UK Privacy Professionals

Independent research conducted by Dimensional Research on behalf of TrustArc





## Table of Contents

- I. Introduction by Chris Babel, CEO of TrustArc. ....3
- II. Survey Methodology & Demographics.....5
- III. General Privacy Results. ....7
- IV. GDPR Results. ....13
- V. Conclusion. ....19

## I. Introduction by Chris Babel, CEO of TrustArc



While security has been a focus of many companies for years and the need to protect and secure information from hackers is as big as ever, privacy is now equally as top of mind for enterprises and managing privacy compliance unlocks data to allow enterprises to drive business value. This includes gaining insight from your customers' data to feed your next marketing campaign, or predicting individual consumer behavior based on understanding clicks on your website.

In order to successfully and legally use data for business purposes, you must comply with a number of state, national and regional regulations. The European Union's (EU) General Data Protection Regulation (GDPR) is increasingly occupying the minds of privacy professionals. In less than a year's time, GDPR, the most sweeping change to data protection in the past 20 years, will go into effect. Its impact will be felt by every organization that does business in the EU, or handles personal information of EU citizens in any manner.

To understand the status of US and UK companies' efforts to meet privacy mandates in general, and in particular to meet the May 25, 2018 deadline for the GDPR, Dimensional Research conducted this research among more than 400 privacy professionals in May - August, 2017, equally split between the US and the UK. I've worked in the privacy and security industry since the 1990's and there are a few findings from the survey that I find particularly interesting and worth highlighting.

### The Job of Privacy is Getting Harder

Among the over 400 US and UK respondents, privacy is the sole job function for 36% of US respondents and 24% of UK respondents. It is an important part (more than 25%) of the job for the remaining US and UK respondents. For the vast majority (over 93%) of US and UK privacy professionals, the job of managing privacy is becoming increasingly complex. Approximately half of US and UK respondents even considered the task as significantly more complex. At the same time, over 94% of all respondents said that the importance of managing privacy is increasing, with over 58% of all respondents expressing that it's becoming significantly more important. For both US and UK privacy professionals, their role is becoming more important while the complexity of their job is increasing. Whether or not that means these privacy professionals feel empowered - or up to the challenge in their roles - is an open question. There's a hint of an answer, though, if we look at the help respondents said they need most in order to comply with GDPR.

### Privacy Pros Need GDPR Planning the Most, and It's Costing Them

US and UK privacy professionals were asked where they needed the most help complying with data privacy requirements. For US respondents, developing a GDPR plan topped the list at 39%, followed by addressing international data transfers (36%) and meeting regulatory reporting requirements (30%). For UK respondents, developing a GDPR plan topped the list at 27%, followed by conducting privacy risk assessments (PIAs and DPIAs) at 26% and addressing international data transfers (24%). A majority of both US and UK respondents haven't yet begun implementing their GDPR readiness plan (61% for US and 64% for UK).

The research honed in on exactly the support these privacy professionals need to become compliant, and the results were: 1) creating new policies and processes (69% for US and 57% for UK), 2) privacy expertise to understand regulations (63% for US and 48% for UK), and 3) technology and tools to automate and operationalize data privacy (48% for US and 50% for UK). For larger US companies with at least 5,000 employees, the need for technology jumped to almost 60% while it stayed the same at 50% for larger UK companies. To find a solution to their GDPR woes, 98% of all of the US respondents and 92% of all UK respondents reported that they will invest in resources such as consultants, new hires and technology to help prepare for next year's May deadline.

## Introduction (continued)

But when we start looking at the financials, it gets really interesting. 47% of US respondents and 31% of UK respondents surveyed say that their overall spending on managing privacy is significantly increasing, while 50% of US respondents and 59% of UK respondents say their spending on privacy management is becoming slightly larger. That means that across the board, investments in privacy are going up.

### GDPR Spending by the Numbers

- 83% of US respondents and 69% of UK respondents expect GDPR spending to be at least \$100,000 (74,000 GBP)
- 40% of US respondents and 25% of UK respondents plan to spend at least \$500,000 (370,000 GBP) to become GDPR compliant
- 17% of US respondents and 6% of UK respondents expect to incur costs over \$1 million (740,000 GBP)

And the bigger the company the bigger the investment:

- 23% of US respondents and 19% of UK respondents with more than 5,000 employees expect to spend over \$1 million (740,000 GBP) on GDPR compliance
- 19% of US respondents and 5% of UK respondents with 1,000-5,000 employees expect to spend over \$1 million (740,000 GBP) on GDPR compliance
- 9% of US respondents and 0% of UK respondents with 500-1,000 employees expect to spend over \$1 million (740,000 GBP) on GDPR compliance to protect consumers and their companies.

### Impact of Brexit and the UK Data Protection Bill on UK GDPR Programs

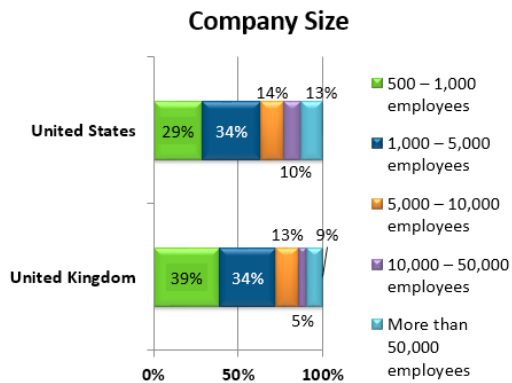
The survey of only UK respondents also indicates that the response to the departure of the UK from the European Union (Brexit) may produce various changes to the GDPR programs of UK companies. 74% of the UK respondents are not reducing their GDPR budgets due to Brexit, while 26% of UK respondents are reducing their investment in GDPR remediation. 32% of UK respondents indicated that Brexit has had no impact on their GDPR programs, but 26% of UK respondents indicated that they were putting their GDPR programs on hold until they could determine the impact of Brexit and the proposed UK Data Protection Bill on the GDPR.

### Conclusion

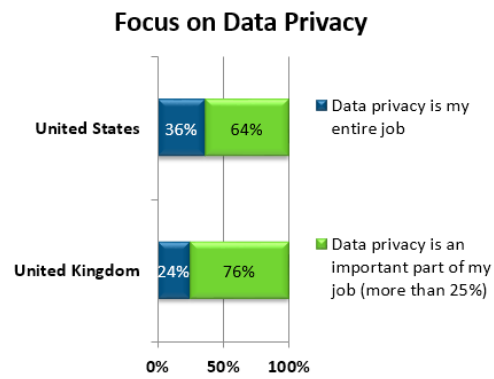
Security has dominated the industry for 20 years for good reason, but with increasingly strict regulations forcing rigid compliance, privacy is bubbling to the top of IT priorities and budgets. These are certainly significant investments and given the complexity of privacy management in general, and GDPR compliance in particular, it's no wonder that privacy professionals need much greater resources to design and deploy processes and technology solutions. This is a clear message that the privacy industry must keep pace with customers and provide the solutions and approaches they need to protect consumers and their companies.

## II. Survey Methodology & Demographics

The online survey was fielded to IT and legal professionals at a fairly evenly mixed target group of small (500 to 1,000 employees), mid-sized (1,000 to 5,000 employees) and large (over 5,000 employees) companies that were subject to the GDPR. A total of 407 US and UK executives, team managers and individual team contributors from companies in the financial services, technology, manufacturing, business services, energy and utilities, healthcare and other key industries completed the survey. The US survey took place in May of 2017 and the UK survey was conducted in August of 2017. Please note that due to rounding, some totals will not sum to exactly 100%.

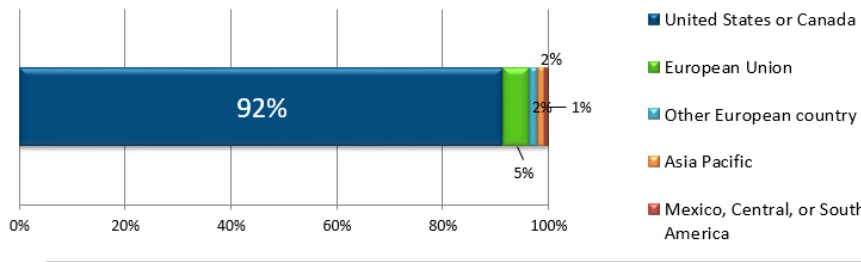


UK respondents weighted more towards smaller (500-1,000 employee) companies (39% UK vs. 29% US)



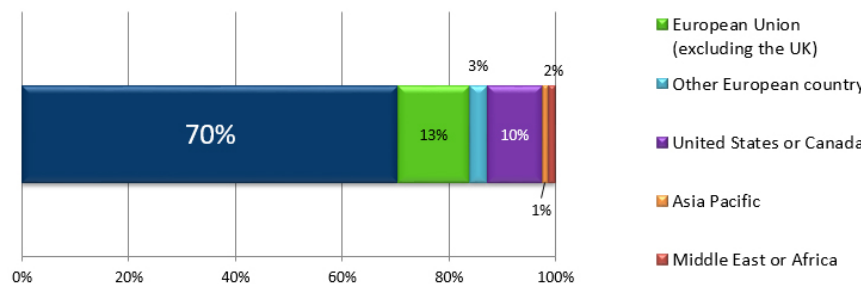
Smaller percentage of UK respondents 100% involved with privacy than US respondents (24% UK vs. 36% US)

92% of the US respondents had US headquarters, while the UK respondents, although primarily based in the UK (70%), also had 30% with headquarters in the EU and other regions.



92% of US respondents have US Headquarters

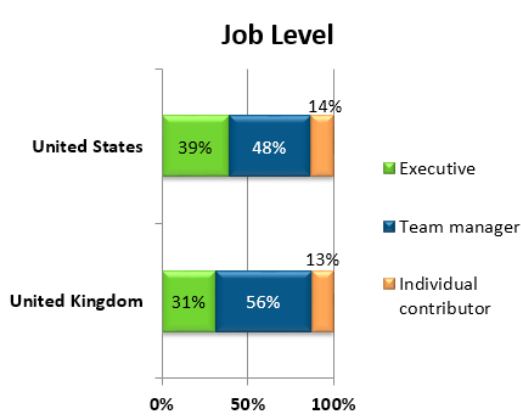
### Corporate Headquarters - United Kingdom



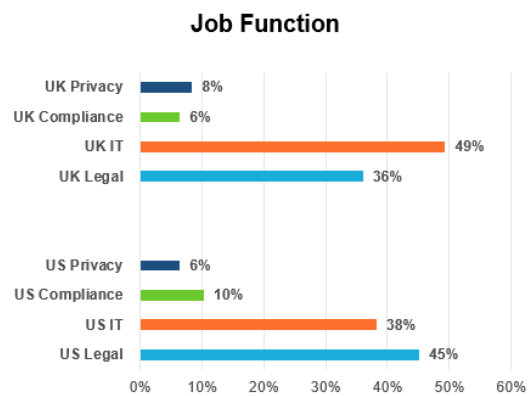
70% of UK respondents have UK headquarters, with 13% having non-UK EU headquarters

\*UK not offered as a separate option in US research

At the US responding companies, the job functions with primary responsibility for privacy ranked by priority were legal (45%), IT (38%), compliance (10%) and privacy (6%). For UK respondents, the job functions with primary responsibility for privacy ranked by priority were IT (49%), legal (36%), privacy (8%) and compliance (6%).

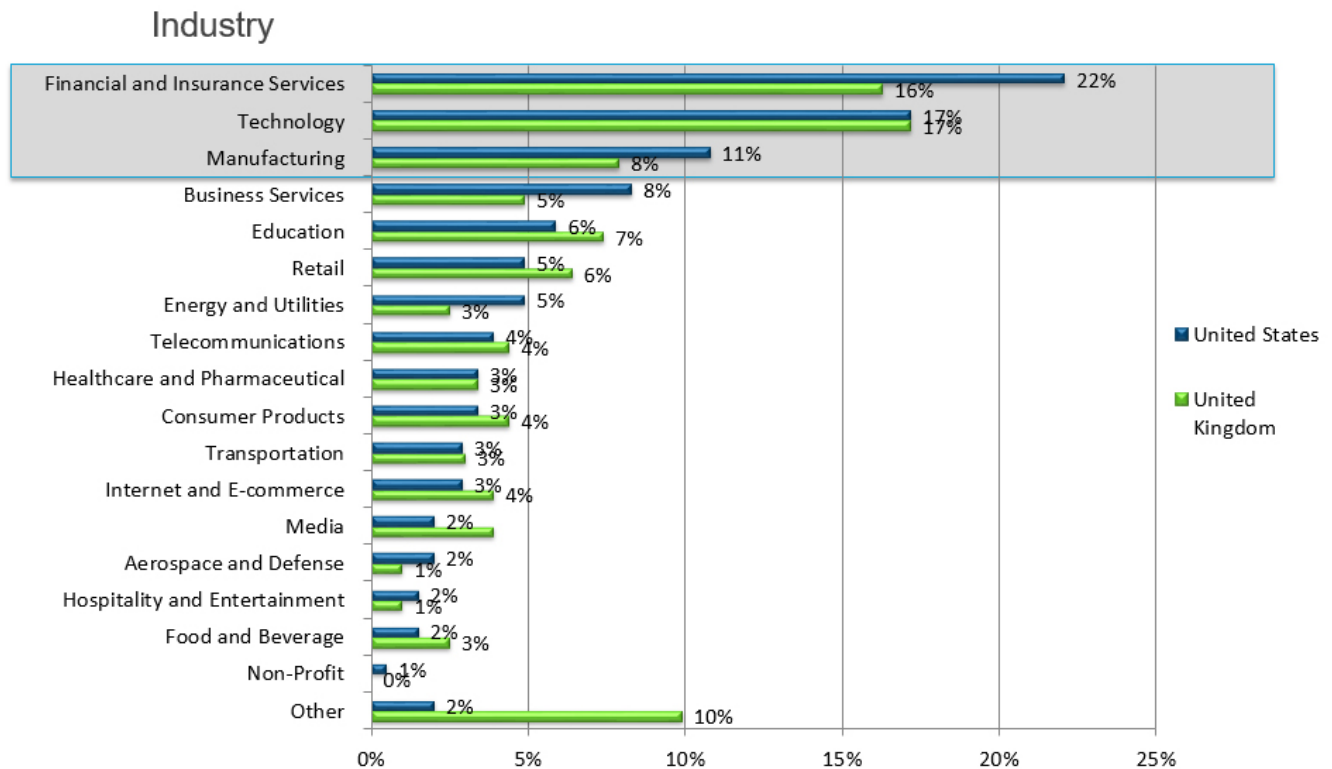


More team managers than executives responded in UK than in US



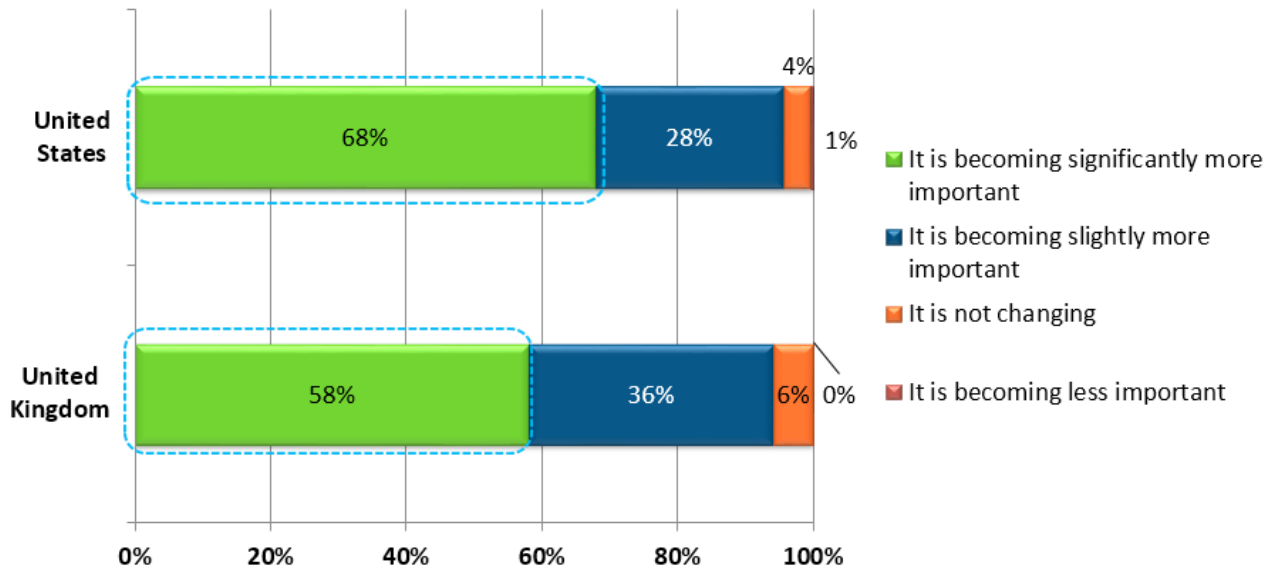
Higher percentage of UK respondents were in IT than in the US

The highest percentage of the individual respondents were in the financial services, technology and manufacturing industries.



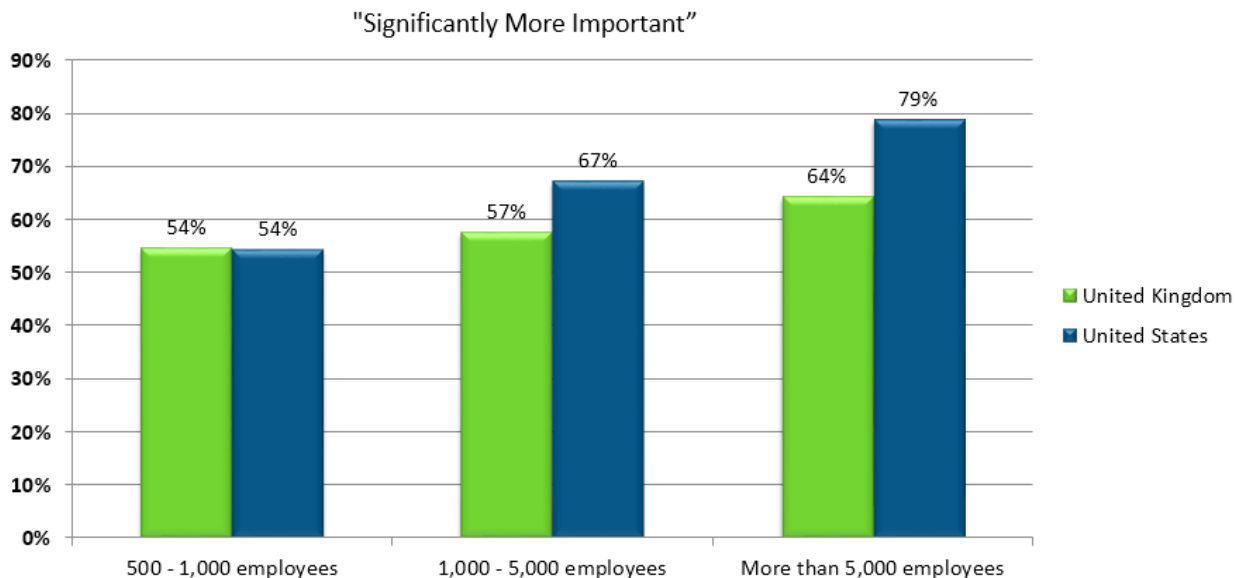
### III. General Privacy Results

Data Privacy Management is Becoming More Important. 96% of US respondents and 94% of UK respondents say that the importance of managing privacy at their company is increasing. Overall, 68% of US respondents and 58% of UK respondents state that managing privacy is becoming significantly more important.



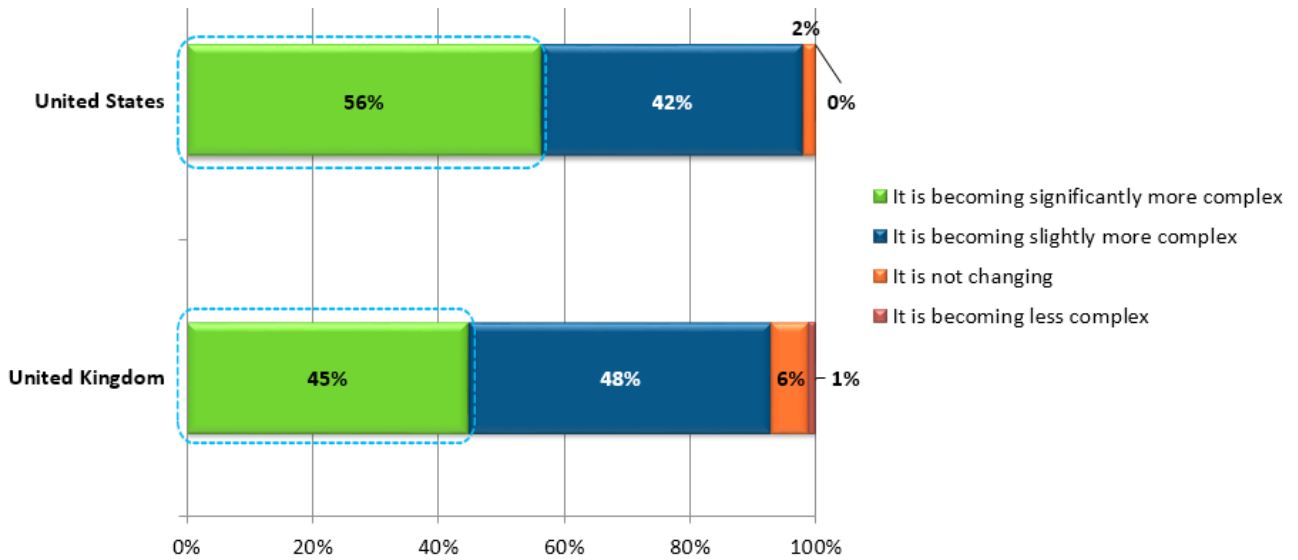
How is the importance of data privacy management changing at your company?

Data Privacy Management Becomes Significantly More Important with Size. Among US companies with 5,000+ employees, 79% state that privacy is becoming significantly more important as compared to 64% of larger UK companies.



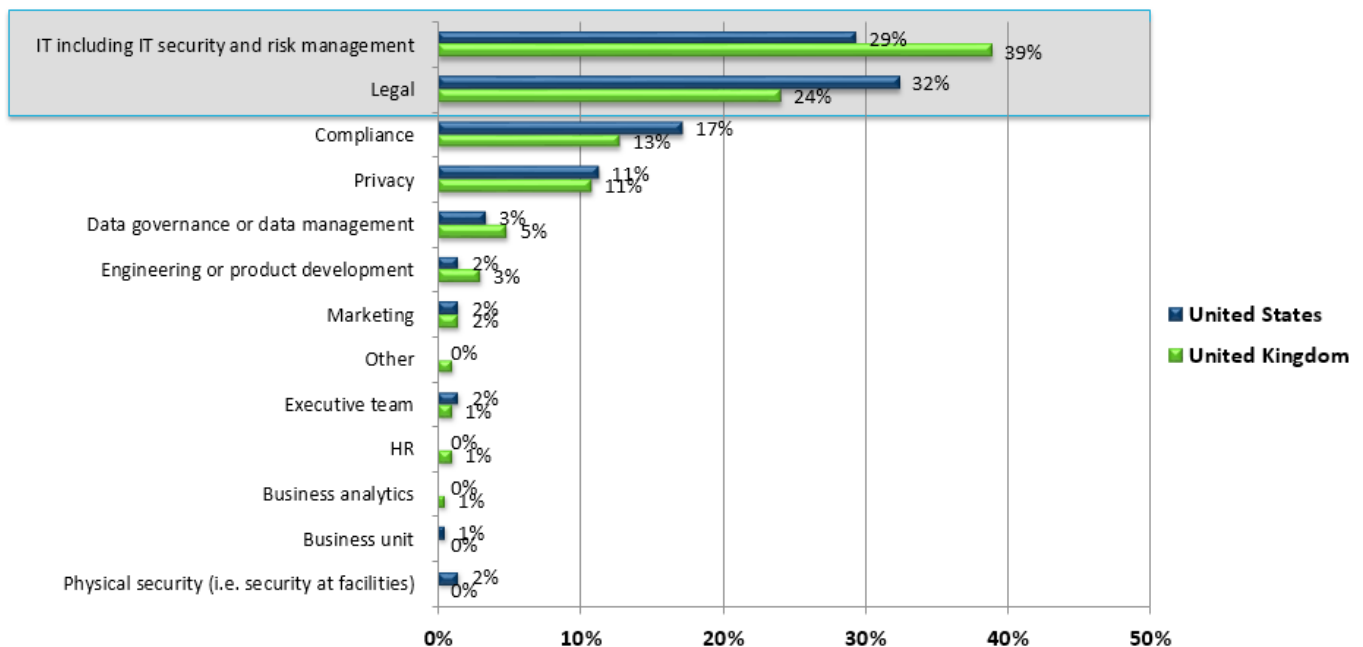
How is the importance of data privacy management changing at your company? (by company size)

**Data Privacy Management is Getting Harder.** 98% of US and 93% of UK respondents say that the complexity of data privacy management at their company is increasing. 56% of US respondents and 45% of UK respondents state that managing privacy is becoming significantly more complex.



How is the complexity of data privacy management changing at your company?

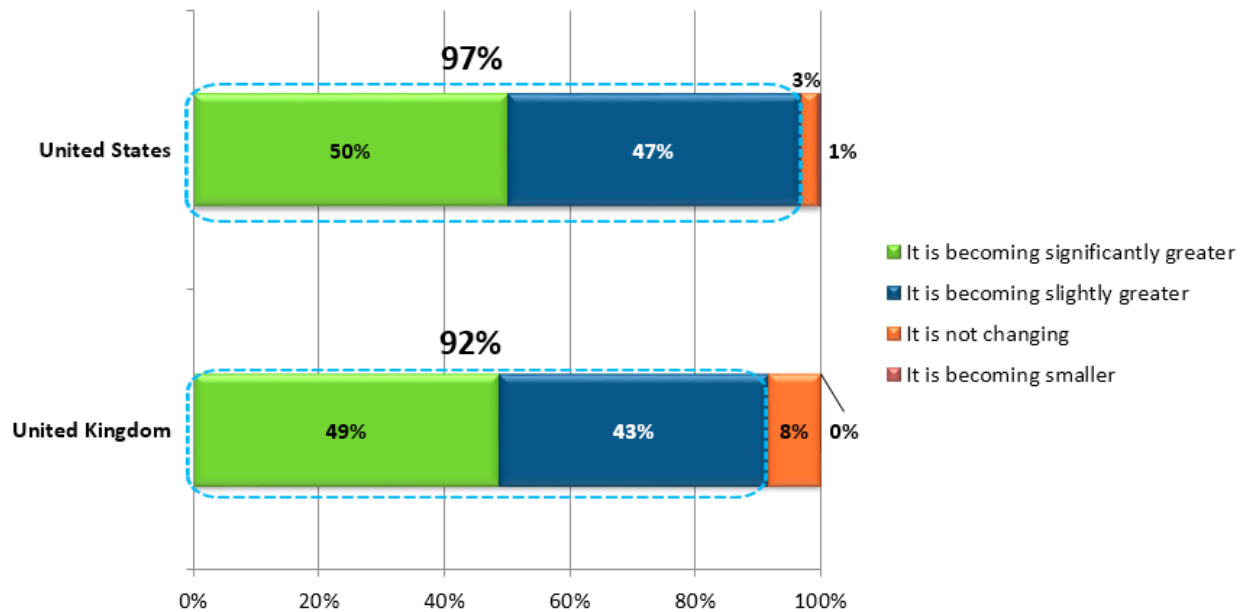
**Multiple Functions Are Responsible for Managing Data Privacy Compliance.** The top job functions involved in managing data privacy compliance at the respondents' companies are legal (primary in US), IT (including IT security and risk management) (primary in UK), compliance, privacy and data governance / data management. The difference in responsibility for GDPR compliance between IT and Legal appears small in the US (32% vs. 29%). However, the difference in the UK is quite large (39% for IT vs. only 24% for Legal).



Which of these job functions has primary responsibility for data privacy and compliance including GDPR at your company?

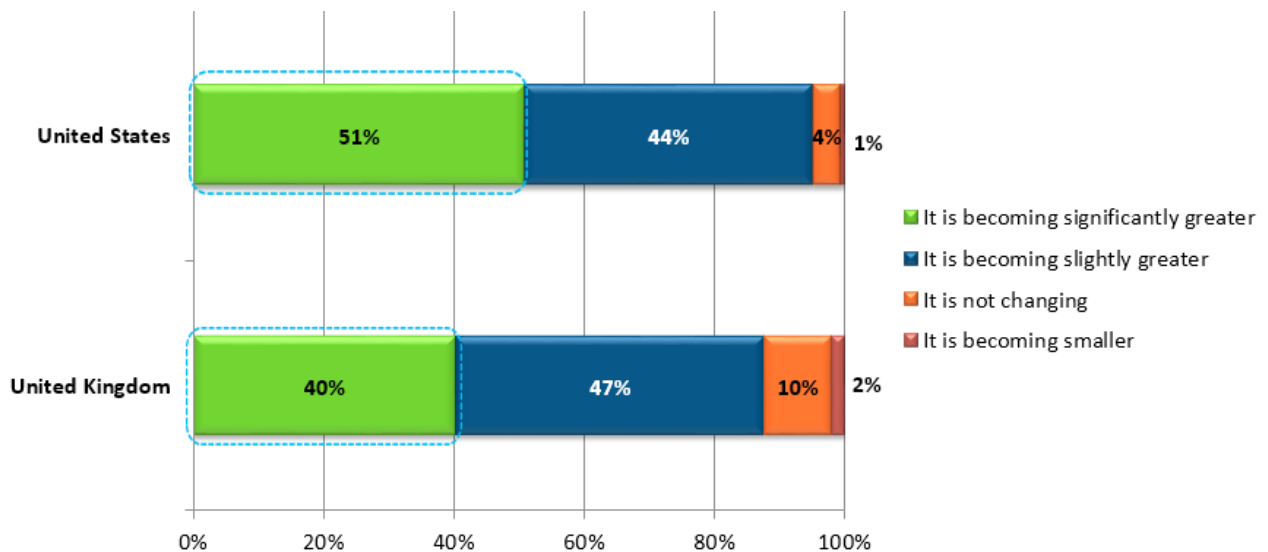


**Data Privacy Management Expertise and Guidance Needs Are Growing.** 97% of US respondents and 92% of UK respondents say the need for expertise or guidance for data privacy management is increasing. About one-half of both US and UK respondents state that the need for expertise or guidance to manage data privacy is growing significantly greater.



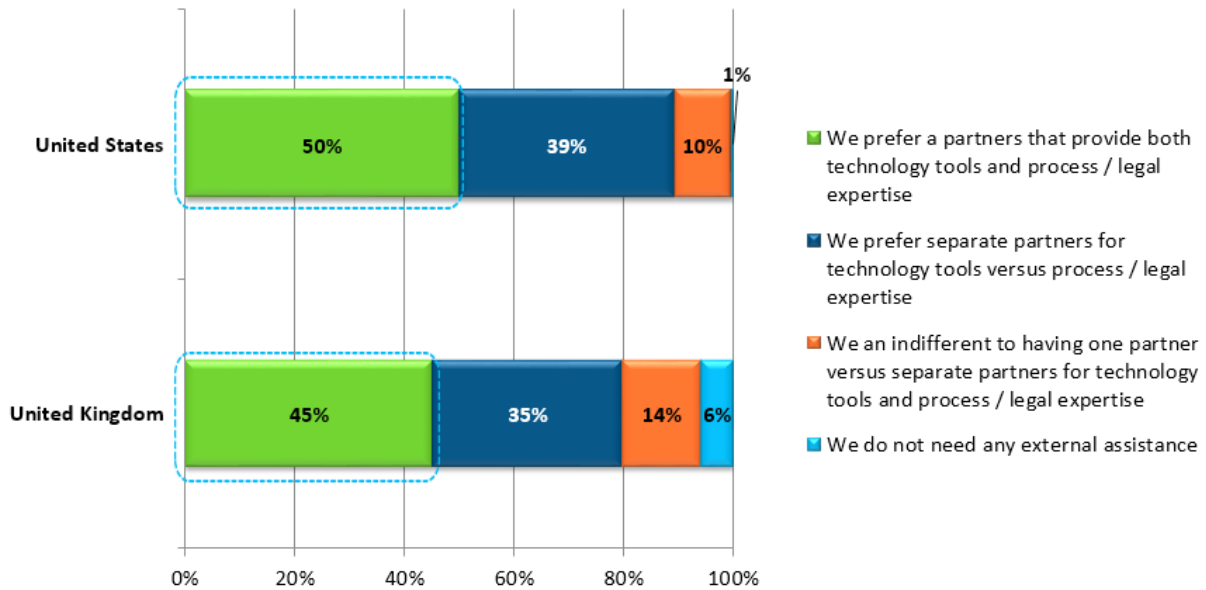
How is the need for expertise or guidance to manage data privacy changing at your company?

**Privacy Technology Needs Are Growing.** 95% of US respondents and 87% of UK respondents say that the need for technology and tools to help manage data privacy is growing. 51% of US respondents and 40% of UK respondents state that the need for technology to manage data privacy is growing significantly greater.



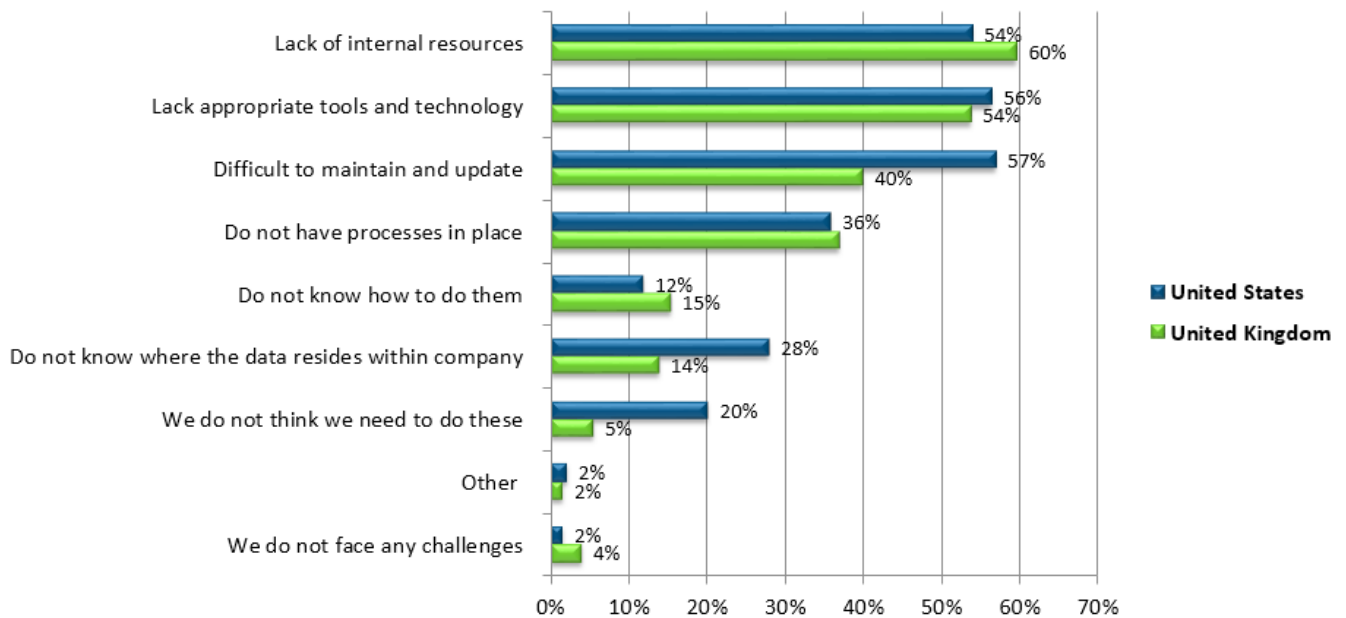
How is the need for technology and tools used to manage data privacy changing at your company?

US and UK Preference for Vendors Offering Both Technology and Expertise. 50% of US respondents and 45% of UK Respondents have a preference for partners that provide both technology tools and process and legal expertise.



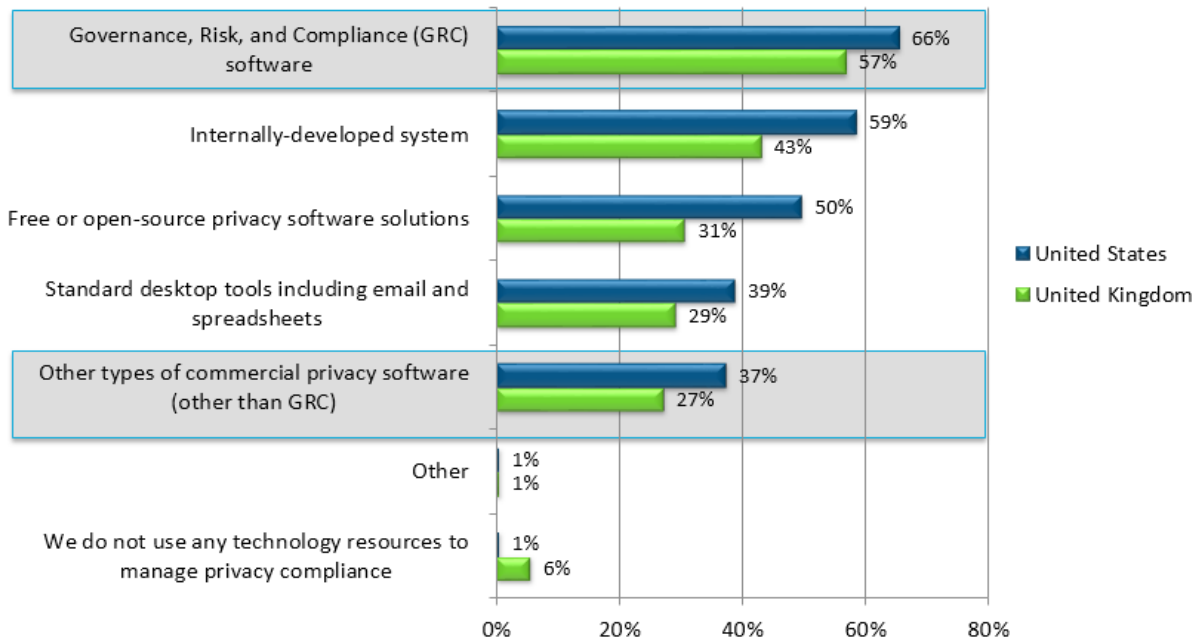
Which of the following statements best represents your company's preferences when evaluating external privacy solutions and resources?

Spotlight on Data Inventory Management. Both US and UK respondents indicate that the top three challenges when managing data inventory and privacy risk assessment are difficulties in maintaining and updating, lack of appropriate tools and technology and lack of internal resources. The number one challenge for US respondents is “difficulty to maintain and update”, while the number one challenge for UK respondents is “lack of internal resources”.



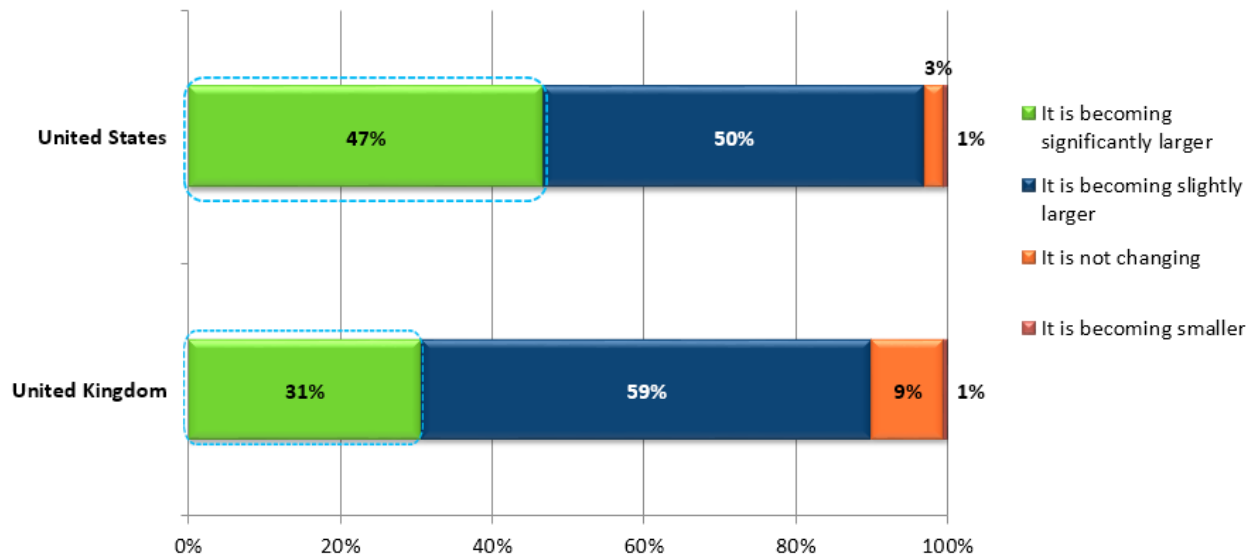
What challenges does your company face when managing data inventory and privacy risk assessment projects?

A Mix of Technology Tools Are Used to Manage Privacy. Governance, Risk and Compliance (GRC) software is the most common resource for both US and UK respondents (66% of US respondents and 57% of UK respondents).



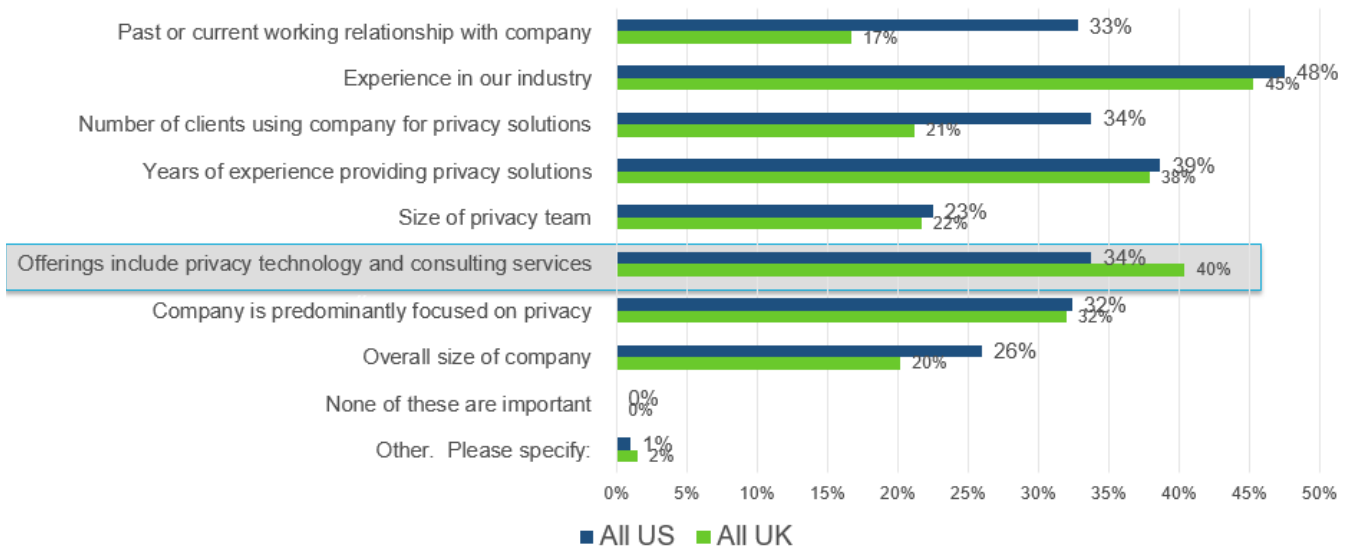
What technology resources do you use to manage privacy compliance at your company?

Data Privacy Management Spending is Increasing. 97% of US respondents and 90% of UK respondents are increasing their investment in managing data privacy. 47% of US respondents and 31% of UK respondents state that their data privacy management spending is becoming significantly larger.



Consider the entire investment your company is making to manage data privacy compliance at your company – including internal and external resources, training, consultants, tools, and all other costs. How is this investment changing?

**Capabilities Sought in a Privacy Partner.** Industry experience tops the list of capabilities that both US respondents (at 48%) and UK respondents (at 45%) sought in an external company or firm that offers technology or consulting solutions for privacy. For UK respondents, offerings including both privacy technology and consulting ranked second (40%), while years of experience in providing privacy solutions ranked third (38%). For US respondents, “years of experience providing privacy solutions” ranked second (39%), while offerings including privacy technology and consulting ranked third (34%).

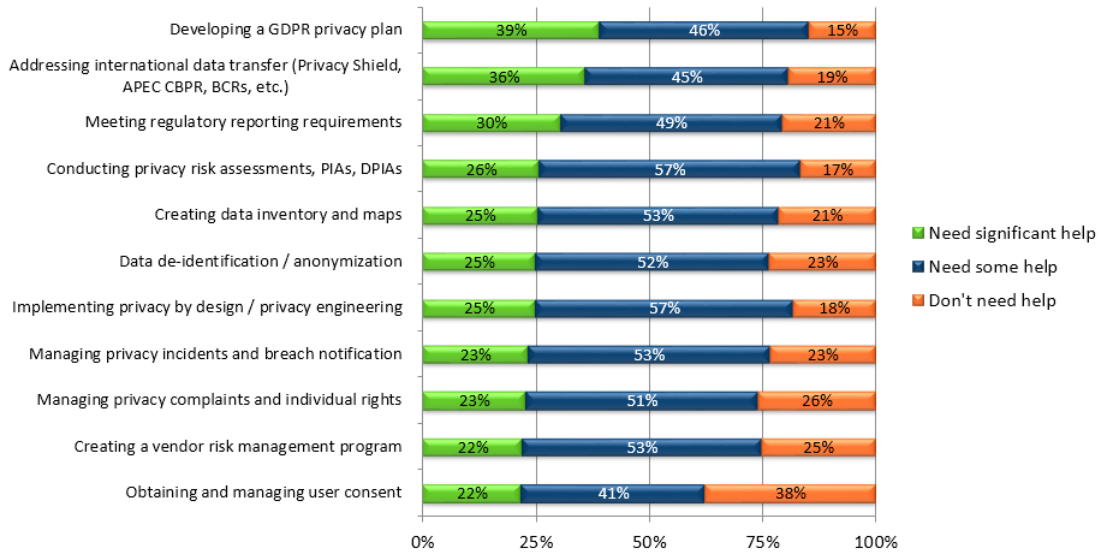


Which of the following qualities are MOST important when selecting an external company or firm that offers technology or consulting solutions for privacy? Choose up to 3 of the following.

## IV. GDPR Results

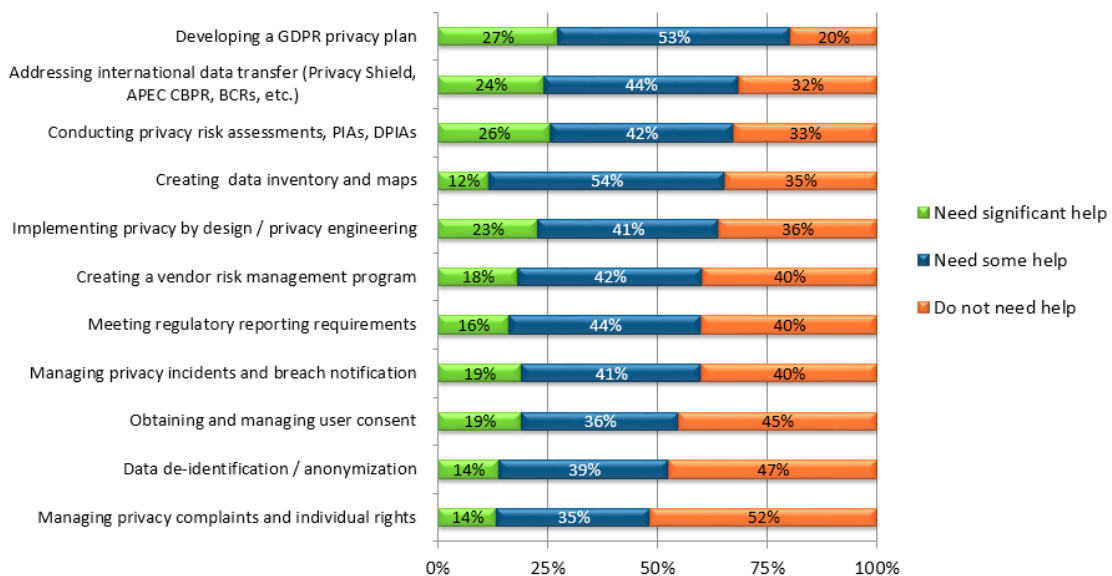
Help is Needed for Data Privacy Compliance Across a Wide Range of Areas, but GDPR Tops the List. Help with the development of the respondents' GDPR privacy plan ranked as the number one need for both US respondents (85%) and UK respondents (80%). For US respondents, the second most important need was for conducting privacy risk assessments, PIAs and DPIAs (83%). For UK respondents, the second most important need was for addressing international data transfers (68%). In general, UK respondents indicated a higher percentage of issues on which they did not need help, than did the US respondents.

### US Respondents:



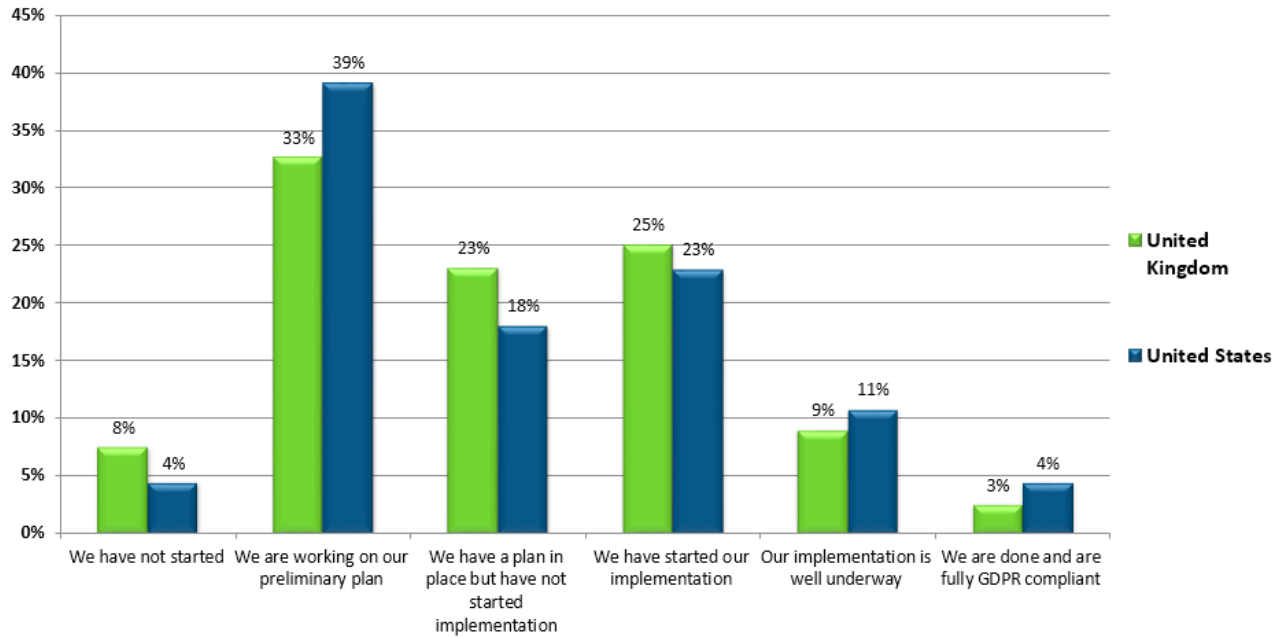
Below is a list of tasks related to data privacy compliance. For each task please indicate the amount of additional help you will need to accomplish these tasks in 2017.

### UK Respondents:



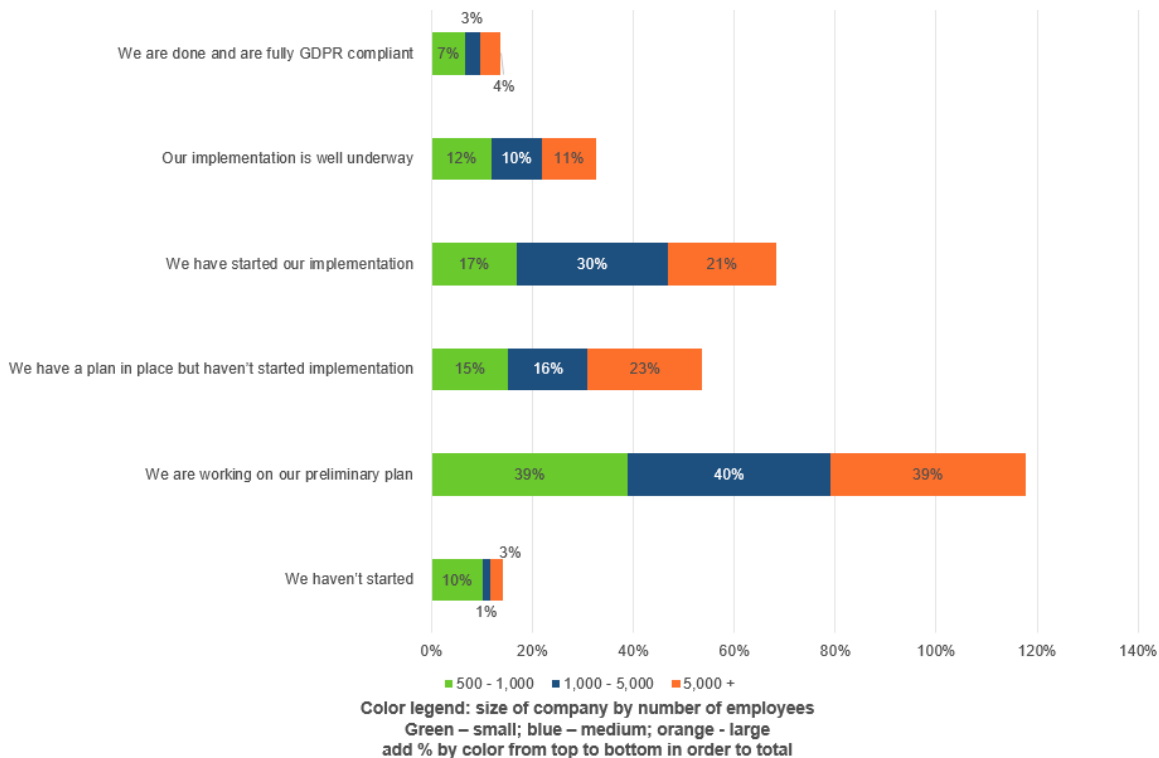
Below is a list of tasks related to data privacy compliance. For each task please indicate the amount of additional help you will need to accomplish these tasks in 2017.

There is a Wide Range of Readiness among the Respondents in Terms of Being Ready for the GDPR May 25, 2018 Deadline. 61% of US respondents and 64% of UK respondents have not begun implementation yet. 43% of US respondents and 41% of UK respondents do not have a full plan. 34% of both US and UK companies are in the implementation phase.

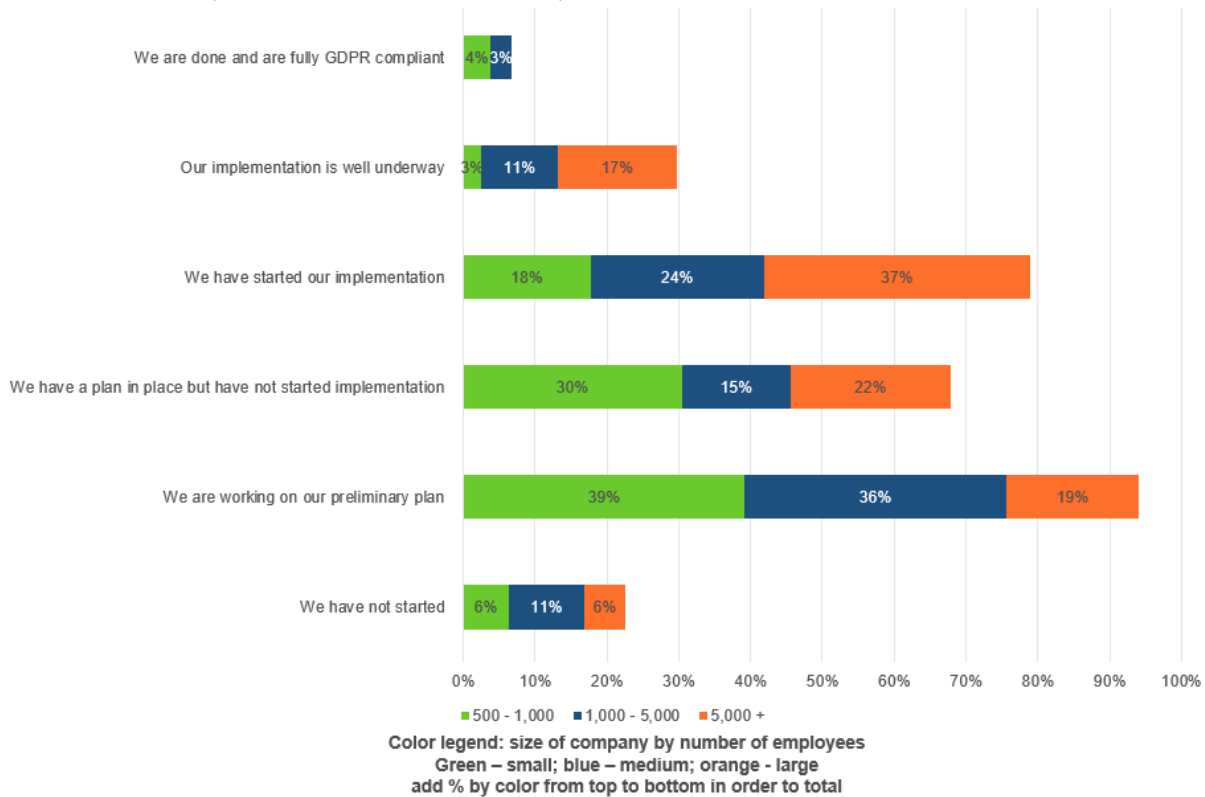


Which of the following best describes the state of your GDPR compliance?

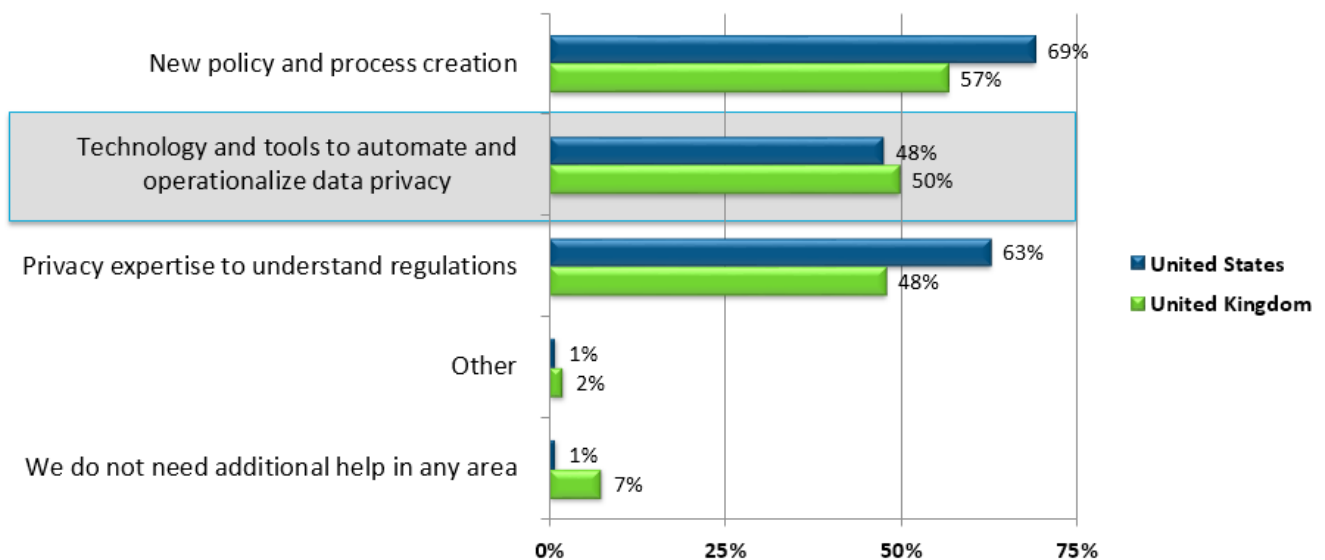
Readiness among US Respondents Ranked by Size of Company. Medium-sized US respondents appear to be most prepared for the GDPR, with 40% in the implementation phase, as compared to only 32% of large companies and 29% of small companies (although a higher percentage of small companies report being done with their GDPR programs (7%) as versus 3% for medium-sized companies and 4% for large companies).



Readiness among UK Respondents Ranked by Size of Company Size. Large UK company respondents appear to be most prepared for the GDPR, with 54% in the implementation phase, as compared to only 35% of medium-sized companies and 21% of small companies.

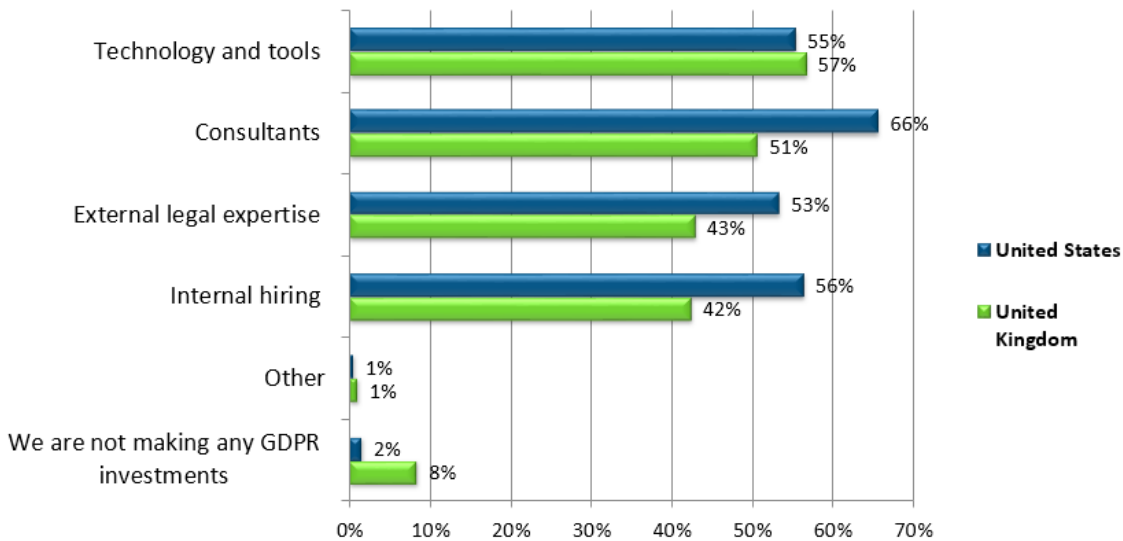


Companies Need a Wide Range of Help With GDPR. 99% of US respondents and 93% of UK respondents report needing additional help with the GDPR. The most help is needed on new policy and process creation (69% for US respondents and 57% for UK respondents). The need for technology help is 48% for US respondents and 50% for UK respondents. 63% of US companies need privacy expertise to understand the regulations, as



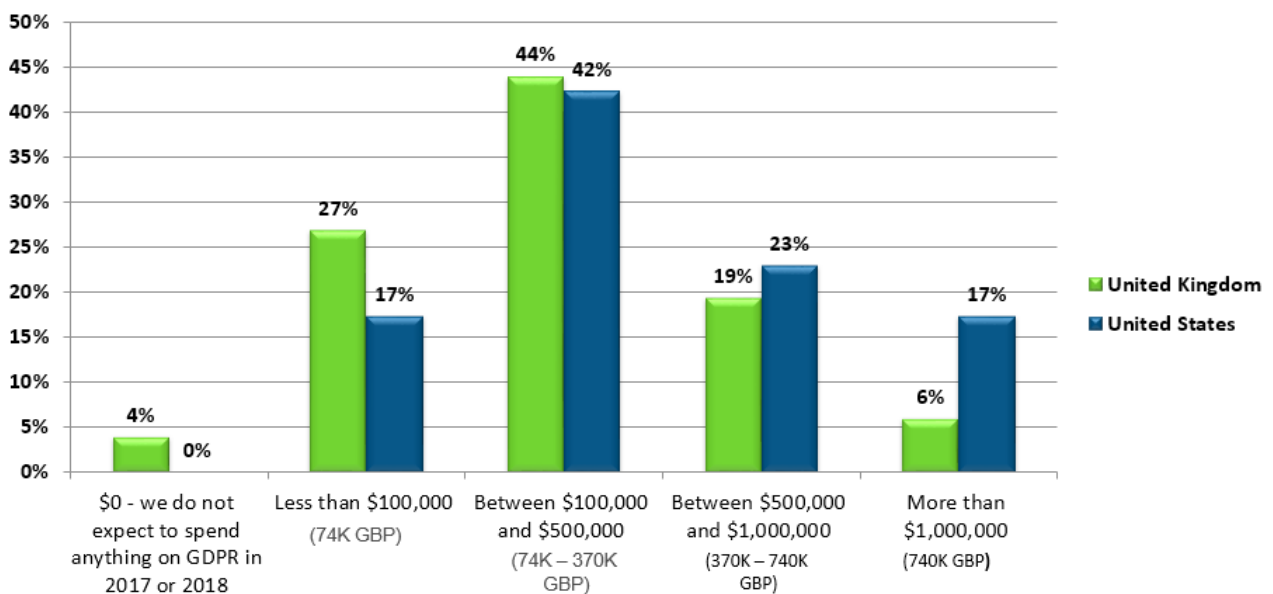
Which of the following areas will you need additional help to meet GDPR compliance in 2017-2018?

GDPR Investments Planned in a Wide Range of Areas. 98% of US respondents and 92% of UK respondents will invest in additional capabilities. The highest overall investment for US respondents is 66% for consultants. The highest overall investment for UK respondents is 57% for technology and tools. 55% of US respondents will invest in technology and tools.



What areas will you be investing in to prepare for GDPR?

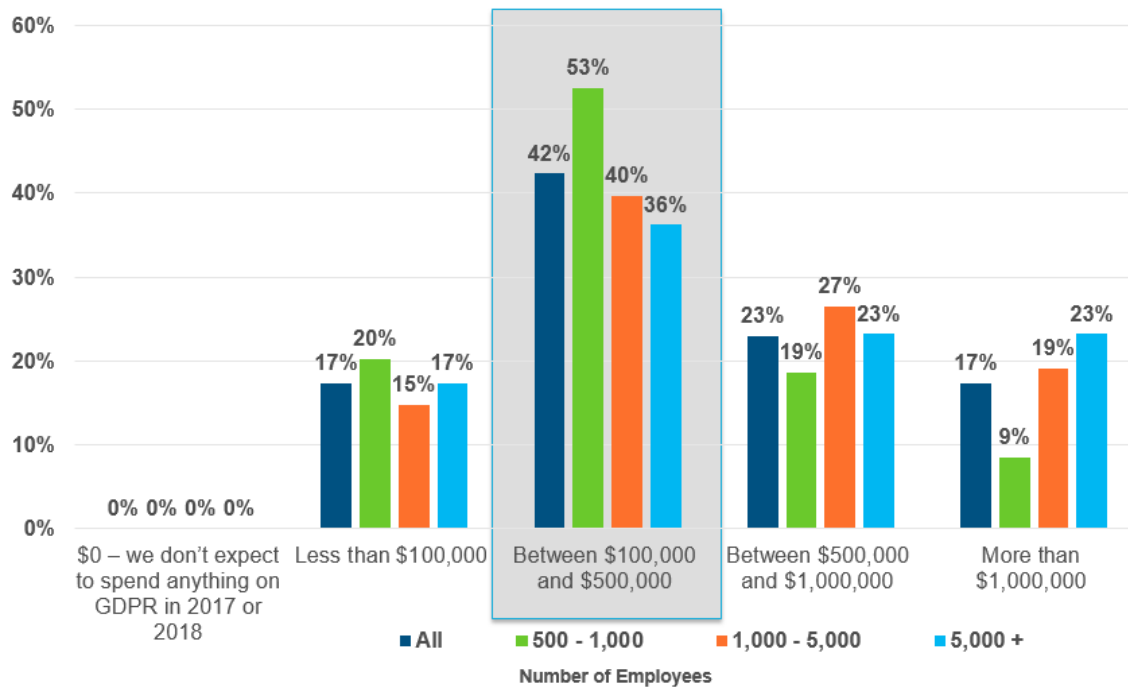
US and UK GDPR Spending. 83% of US respondents expect to spend over \$100K (74,000 GBP) on GDPR-related compliance expenses in 2017-2018. 40% of US responding companies plan to spend at least \$500K (370,000 GBP) on GDPR expenses. 17% plan to spend over \$1 million (740,000 GBP) on GDPR-related expenses. 69% of UK respondents expect to spend over \$100K (74,000 GBP) on GDPR-related compliance expenses in 2017-2018. 25% of UK responding companies plan to spend at least \$500K (370,000 GBP) on GDPR expenses. 6% plan to spend over \$1 million (740,000 GBP) on GDPR-related expenses. To account for rounding, some figures have been adjusted in order for the totals to equal 100%.



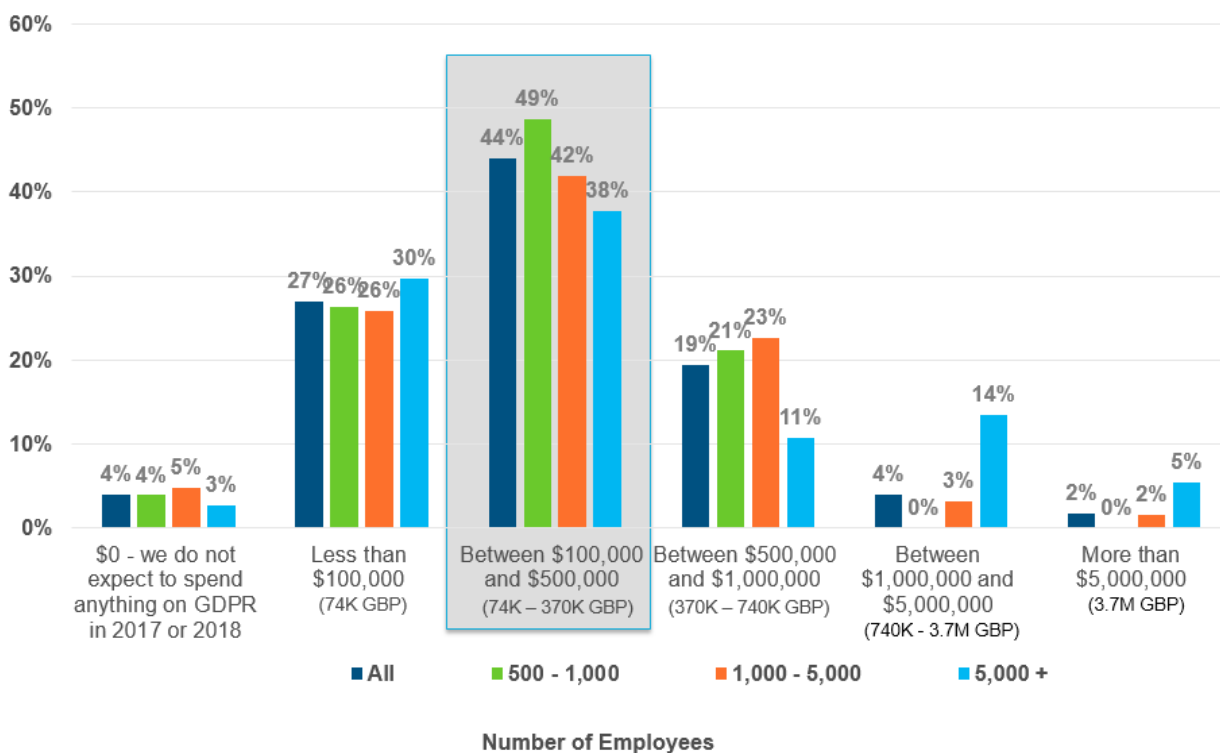
Approximately what is your company's overall expectation for GDPR-related privacy compliance expenses in 2017 and 2018? Include all internal and external personnel, training, consulting, legal advice, technology, tools, and other costs in your estimate.



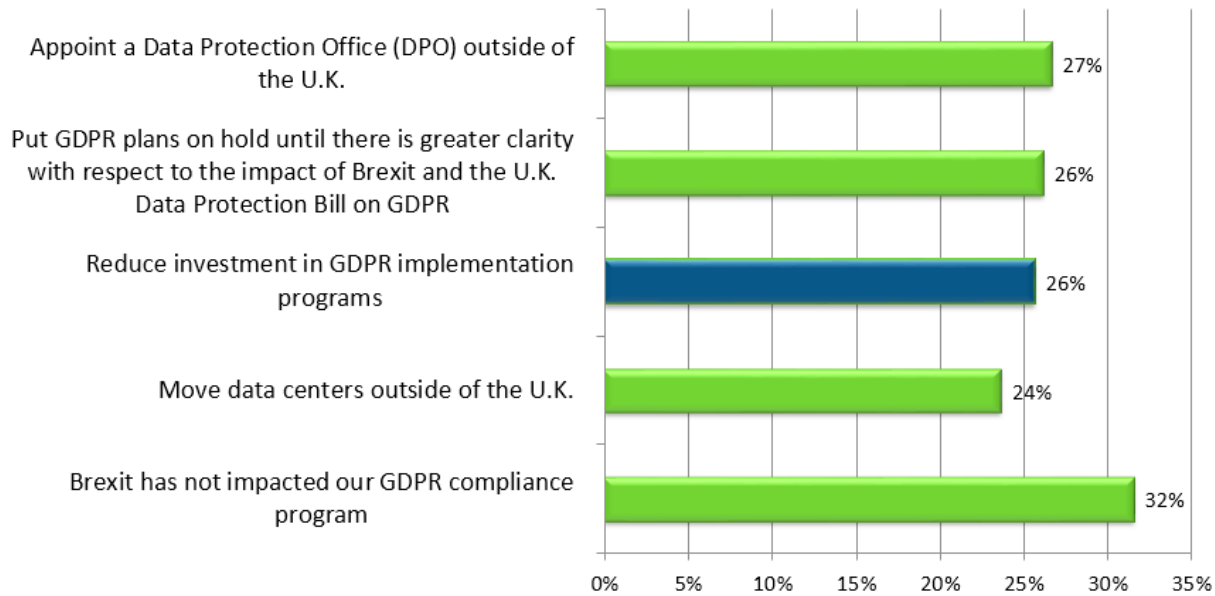
**US GDPR Spending by Size of Company.** The bulk of US respondents' GDPR budgets were in the \$100,000 to \$500,000 range, irrespective of company size. 9% of small US companies, 19% of medium-sized companies and 23% of large US companies are spending over \$1 million.



**UK GDPR Spending by Size of Company.** The bulk of UK respondents' GDPR budgets were in the \$100,000 to \$500,000 (74,000 – 370,000 GBP) range, irrespective of company size. No small UK companies were spending over \$1 million (740,000 GBP). 19% of large UK companies were spending over \$1 million (740,000 GBP), with 5% of large UK companies spending over \$5 million (3.7 million GBP).



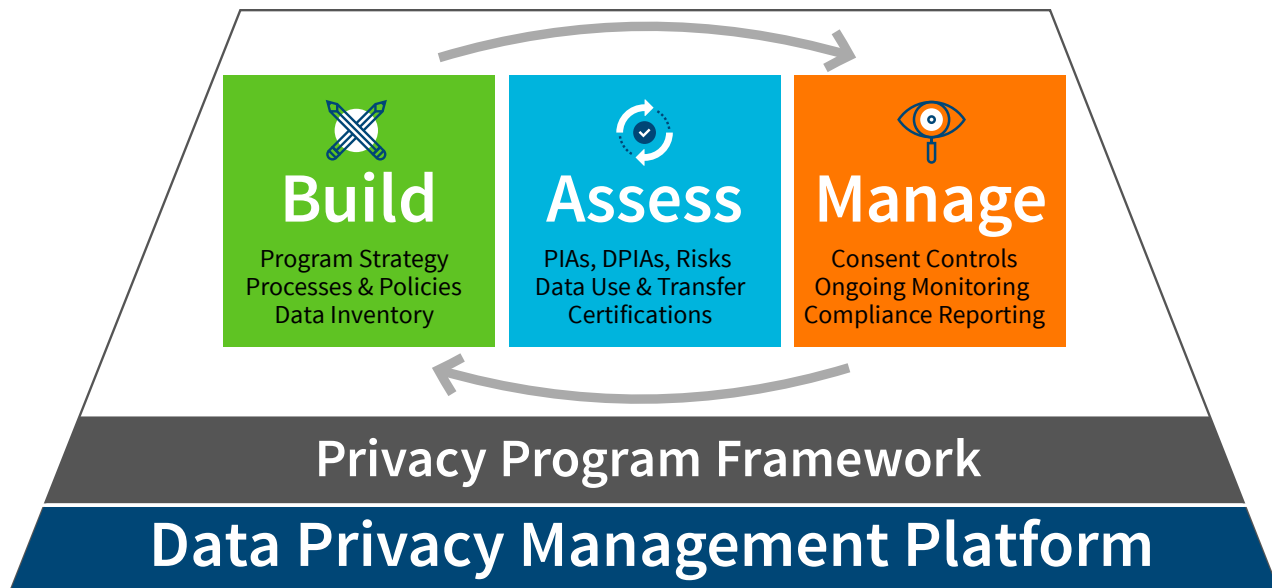
Three out of Four UK Respondents Not Reducing Their GDPR Budgets Due to Brexit. 74% of the UK respondents are not reducing their GDPR budgets due to Brexit, while 26% of UK respondents are reducing their investment in GDPR remediation. 32% of UK respondents indicated that Brexit has had no impact on their GDPR programs, but 26% of UK respondents indicated that they were putting their GDPR programs on hold until they could determine the impact of Brexit and the proposed UK Data Protection Bill on the GDPR.



Has your company changed or considered changing any plans for GDPR as a result of Brexit?  
(Question for UK Respondents only)

## V. Conclusion

As is evident from this survey, data protection management and compliance with the EU GDPR in particular can prove to be a daunting task. However, TrustArc has a comprehensive set of privacy management solutions to help you manage your data privacy management program. We have solutions to help you with all phases of GDPR compliance. Our solutions are powered by the TrustArc Platform, along with our team of privacy experts and our proven methodology. For further information on the TrustArc Platform, just go to our website at [www.trustarc.com](http://www.trustarc.com).



## About TrustArc

TrustArc powers privacy compliance and risk management with integrated technology, consulting and TRUSTe certification solutions – addressing all phases of privacy program management. Our new name, TrustArc, reflects our evolution from a certification company into a global provider of technology-powered privacy compliance and risk management solutions. The foundation for our solutions is the TrustArc Privacy Platform, which provides a flexible, scalable, and secure way to manage privacy. Our technology platform, fortified through six years of operating experience across a wide range of industries and client use cases, along with our services, leverage deep privacy expertise and proven methodologies, which we have continuously enhanced through thousands of client projects over the past two decades. Headquartered in San Francisco, and backed by a global team, we help over 1,000 clients worldwide demonstrate compliance, minimize risk, and build trust.

## About Dimensional Research

Dimensional Research, based in Sunnyvale, California, is a market research firm that specializes in practical research services for technology companies. Dimensional Research clients represent a wide range of the most successful technology organizations — from start-ups to Fortune 500 companies. Its clients offer technology products and services used by IT teams, business stakeholders, consumers, developers and everyone in between.