



TrustArc 2020 Global Privacy Benchmarks Whitepaper

Table of Contents

Introduction	3
Executive Overview	4
Three key developments	5
A global view from top to bottom	6
Benchmarking privacy: Key organizational differences	7
Analysis and Insights	8
Privacy measures being undertaken	8
Organizational commitments to privacy	9
Perceptions of confidence	11
The most challenging elements of privacy management	12
Regulatory knowledge, impact and compliance	12
Solutions and their effectiveness	13
Budgeting for privacy	16
CCPA readiness	16
Pandemic impact on privacy	18
New technologies	19
Conclusion	20

Introduction

Privacy and data protection have become cornerstones of good governance, a tenant that most companies now publicly espouse. When stakeholders, from investors to consumers, embrace Environmental, Social, and Governance (ESG) practices as an essential standard of trustworthy corporations, executives no doubt want to be viewed as beyond reproach on any matters concerning privacy and data protection practices. Setting exemplary standards is not easy. Plotting a course through new risks to privacy and data protection security in an increasingly digitized world while staying abreast of a growing global patchwork of regulations presents a complex navigational challenge.

To capture the challenges and the *opportunities* that have arisen in data protection and privacy, TrustArc inaugurated an annual [Global Privacy Benchmarks Survey](#) in 2020. A range of crucial stakeholder opinions were gathered. In total, more than 1,500 senior executives, privacy office leaders, privacy team members, middle management, and full-time employees outside the privacy function were surveyed.

The findings in this report captured:

- Decision-making and strategic approaches to data security and privacy
- Approaches to the most challenging elements of privacy management
- Preparedness to address privacy and security risks, including budgets
- CCPA compliance readiness and critical challenges
- Impact of COVID-19 on privacy
- Impact of adoption of new technologies on privacy

In a year where so much had been upended, one key finding emerged that was heartening: enlightened leaders found transformative opportunity. Akin to other fundamental business principles such as having a “safety mindset in everything we do” or setting an industry’s “highest quality standards,” forward-thinking enterprises were tackling data protection with similar mindfulness and making data privacy a core operational and philosophical focus for their business.

The implications for all enterprises were clear. With a growing list of regulations around the globe, enterprises need to stay current and manage their risk -- not only reducing exposure to data breaches and lawsuits -- but, just as importantly, to safeguard their public reputation.

Executive Overview

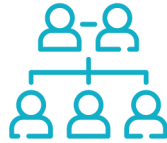
To tackle their data security and privacy needs, companies globally employed a range of measures. Staying on top of new regulations, especially CCPA, were top priorities for companies when asked about changes underway or asked separately what new initiatives they are undertaking. **To get the job done, training was a clear priority.** The COVID-19 pandemic did not change this focus; it has amplified it. Here is a snapshot of what was found:

Many of the findings were positive.



Privacy is a clear differentiator.

81% say privacy is a clear differentiator for their company, and 90% say their company is mindful of privacy issues.



A similar positive finding exists between employees feeling **empowered to raise privacy issues without reprisal (90%)** and their clarity of understanding of what to do on day-to-day privacy issues (83%).



Self-reported knowledge about regulations is generally good, but not great, although not surprisingly, **this is higher among privacy leaders and their team members.**

Not all of the findings were comforting.

1/4 said they were not confident in their company's privacy approach - a sizable level of skepticism.

Confidence was at its lowest when assessing the general public's confidence in their companies, with 36% expressing a lack of perceived confidence. When lacking confidence, the biggest culprits were in breach reporting and leadership.

Further, companies lagged on the road to CCPA compliance, with slightly over half (53%) having not started any implementation. In a world where simply knowing about regulatory frameworks and being on the way to compliance is not enough, this finding was concerning.

Just slightly more than one in three (36%) companies used purpose-built, automated software solutions to tackle these issues. Where solutions fell short, it was because they were not automated. It was difficult to track and make changes and to do so in dynamic and complex environments.

Stakeholders from all sides recognize that privacy requires significant ongoing investment. Meeting new regulatory standards at the same time as staving off the threats of a global pandemic made clear that privacy is never "done." **Automation, expert advice, and commitment from top to bottom of an organization remain essential.** High tech, high smarts, and high standards are needed to build transparency, accountability, and compliance in today's privacy world.

Three key developments

01

California Consumer Privacy Act

The birthplace of digital innovation, Silicon Valley, became home in 2020 to the globe's most far-reaching data legislation, the California Consumer Privacy Act (CCPA). After decades fixated solely on how to monetize customer data, enterprises were tasked with figuring out how to protect and, in many cases, remove data entirely. Transparency emerged as a core corporate principle, with actionable obligations under the CCPA to codify how personal consumer information is used and limit its selling. As many enterprises scrambled to comply, others seized the opportunity to emerge as customer advocates and brand leaders in good governance.

02

Next-Gen Technologies

Artificial intelligence (AI) and machine learning (ML) technologies accelerated business innovations, advancing the holy grail of one-to-one communication and experience delivery to customers. Being exceptional at helping businesses "*make it easy like you know me*" also created a converse effect: the challenge of "*protect me like we never met.*" Nonetheless, some companies leveraged these innovations to help them become improved privacy stewards.

03

COVID-19

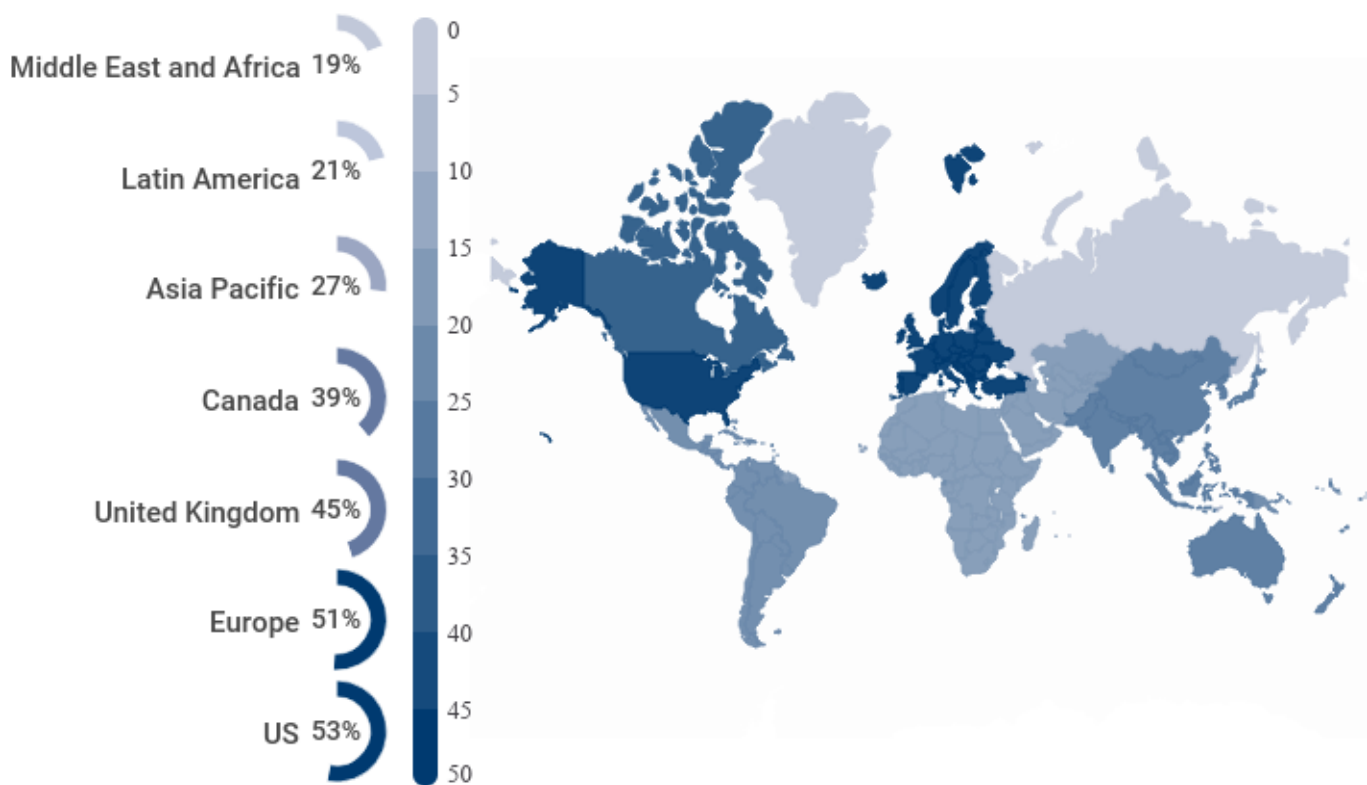
2020 will forever be known as the year of the Pandemic. COVID-19 upended major industries; almost every business had to readjust its operations. For industries hard hit, many initiatives fell by the wayside, including privacy efforts. Yet many enterprises in the digital world thrived, with a concomitant need to increase resources and budgets dedicated to data protection and privacy.

A global view from top to bottom

Over 1,500 respondents from around the globe -- including senior leadership both in and outside the privacy office, privacy officers, middle management, and full-time employees -- made this report possible by offering up their candid views on how well their enterprises managed data protection and privacy.

Participants came from companies with head offices located in North America, UK, and Europe. Their companies operated globally – not only in their country of origin but also in Asia Pacific (27%), Latin America (21%), and the Middle East and Africa (19%). Of those operating in the United States, most had operations in both California and New York. For head offices in Europe, the UK, Germany, and France were the most common operating countries.

Figure 1: **Operating Regions/Countries**



The survey represented a wide range of industries. The most prevalent were technology, manufacturing, financial services, retail, and health care. Over three-quarters of respondents were from firms with annual revenue over USD 500M, almost half exceeded \$1B, and 23% exceeded \$5B.

Nearly two-thirds (64%) indicated that they have a privacy team office function at their company. Of those in a role related to a privacy office or team, 30% were the privacy lead, and 22% had executive oversight.




Benchmarking privacy: Key organizational differences

In total, we obtained 21 ratings on privacy attitudes and opinions from a cross-section of organizational roles around the globe. To build stand-out privacy competence, companies need dedicated internal experts very knowledgeable about their company's applicable regulations coupled with widespread employee understanding and preparedness for their roles in ensuring privacy compliance.

With these in hand, we observed significant differences across various organizational roles.

- Senior executives tend to view their enterprise's privacy approaches quite positively.
- Middle management views their companies as doing "average."
- Employees outside the privacy function slightly less so.
- **By strong contrast**, privacy executives and privacy team members had more negative views of their company performance. It was not surprising to see privacy teams being hard on themselves and pushing themselves to do better in light of a myriad of challenges facing these teams.

Perhaps unsurprising, the responses also diverged when it came to company size.

 <p>Small</p>	<p>Respondents from small companies believe their approaches are effective, managing privacy with a hands-on, direct approach. As changes to privacy regulations occur, their ability to adapt is a strength.</p>
 <p>Mid-sized</p>	<p>Mid-sized companies struggle the most. Scaling inevitably means re-tooling processes and technology, along with organizational approaches. Many lack the right technology solutions and automation.</p>
 <p>Enterprise</p>	<p>Large enterprises are more likely to have mature organizational processes and practices to wrap data privacy and practice in. They also, of course, tend to invest more in mature and automated technology solutions.</p>

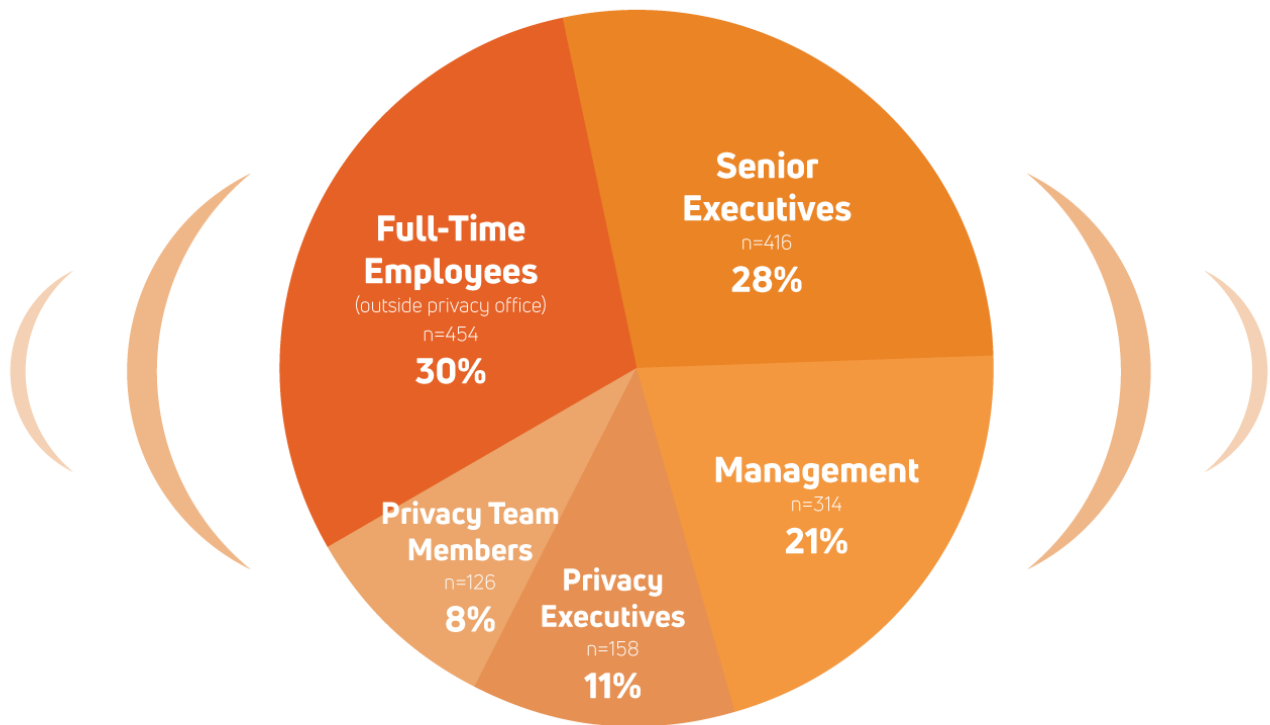
Analysis and Insights

Privacy measures being undertaken

Looking at organizations' top initiatives and the changes afoot in 2020, the results were consistent and clear. Adapting to new regulations and adjusting privacy and data protection policies are top priorities for companies going forward. Additionally, respondents indicate a strong affinity for training staff, which we know not only helps ensure compliance with new regulatory requirements but also reduces human error.

Not surprisingly, priorities varied by role, with privacy-related roles more focused on the nuts and bolts of operational practices. For instance, we noted the following.

Figure 2: **Percent Who Chose “Adjusting Transparency” as the #1 Initiative for 2020***



Clearly, individuals tasked with getting the job of “privacy” done saw a large part of their role as increasing the data protection transparency of their organization to the world.

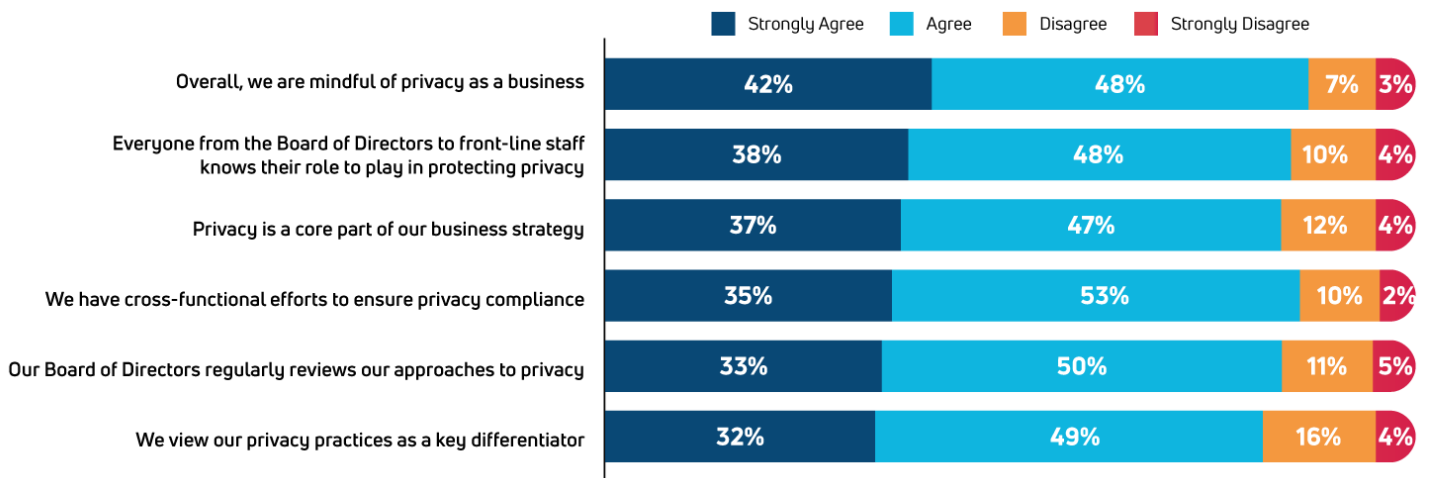
Organizational commitments to privacy

Adapting to these new realities required companies to reconsider their business strategy versus simply taking a “check the box” approach. A prior survey of privacy professionals determined evidence that this shift was underway in 2020, 70% of whom believed privacy had become an integral part of overall strategy and business planning and that it would become increasingly embedded into business operations.¹ Our survey reinforced this view and shed further light on it.

More than 9 out of 10 believed their organization was mindful of privacy as a business. On all other critical measures shown below, more than 8 out of 10 viewed their company positively when it came to serious approaches to privacy at all levels of the company.

Nonetheless, there was a gap with some 20% not viewing privacy practices as a critical differentiator, double that of the 10% of skeptics who did not believe their company was mindful of privacy.

Figure 3: **Organizational Commitments to Privacy**



Privacy Function

Paradoxically, much of this skepticism comes from the privacy function itself. 28% of privacy executives and 30% of privacy team members *disagree* or *strongly disagree* that their company’s privacy practices are a key differentiator. While this may be because of their greater insight into the details and shortcomings of the organizations they work for, it may also come from a sort of “clinical bias” that results from working only with the difficult circumstances of constantly adjusting requirements.

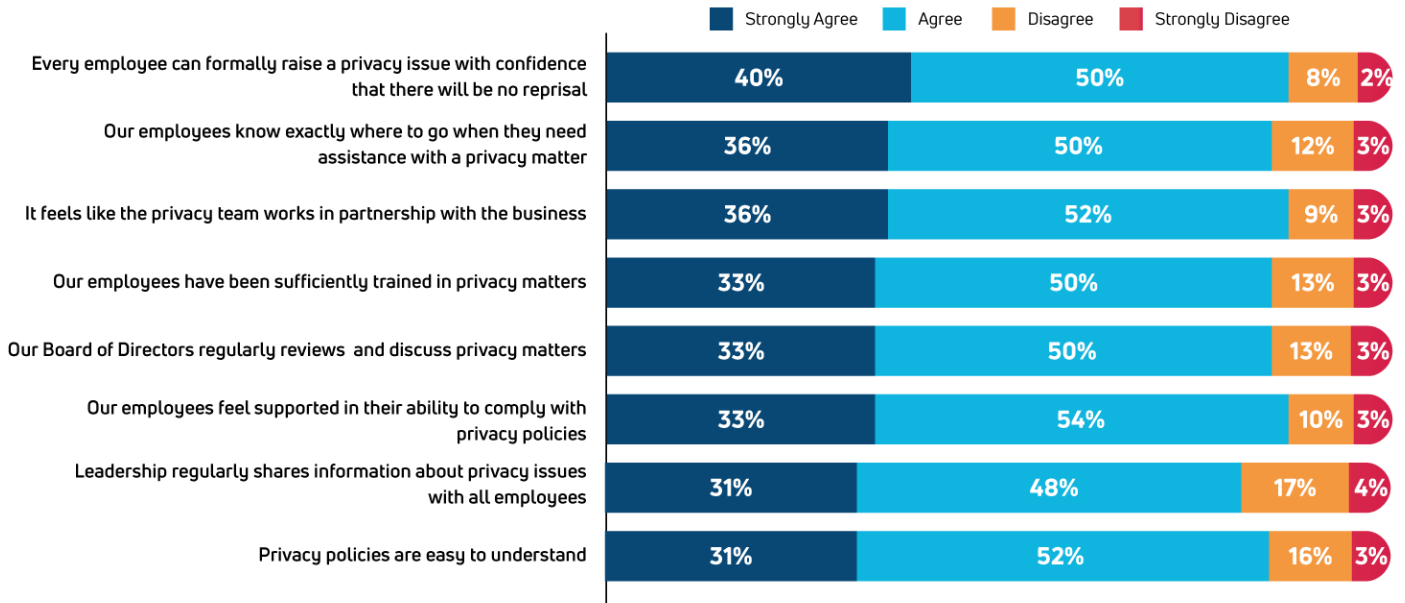
Senior Executives

Senior executives, who see privacy and data protection challenges being met satisfactorily, are pleased. Those who work directly in the privacy program may complain of the difficulty in getting the job done and attribute that to a lack of organizational commitment. **Executives, by contrast, tend to see the resources and effort to do the oft-times difficult work of privacy as evidence of their commitment.**

¹ Nymity (now TrustArc). (2019, July). “Privacy Pulse.” 1-9.

In day-to-day approaches to managing privacy, we found positive results, with 9 out of 10 reporting no fear of reprisal in raising a privacy issue. The vast majority claim to know where to go when they need assistance and that their privacy team is a partner (not a rival or opposing interest) in the business (see highlight in the graph below). There is a modest but notable drop to 83% who believe that their company’s privacy policies are easy to understand.

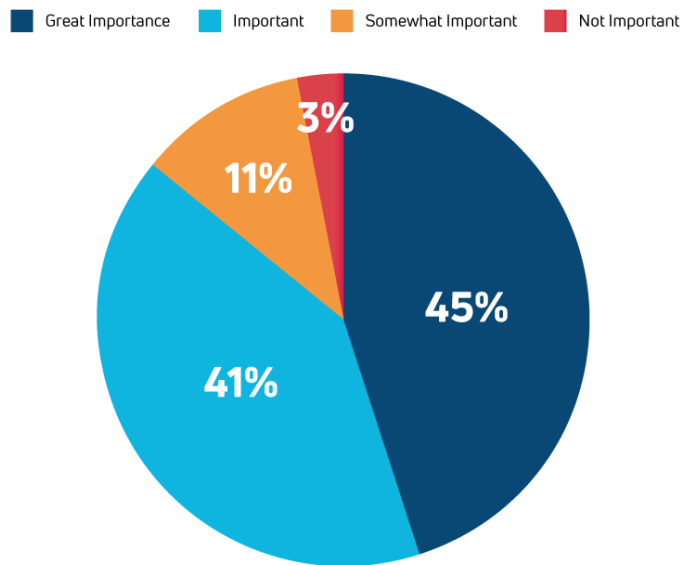
Figure 4: **Organizational Approaches to Privacy**



Again, those tasked with getting the job done may have more significant skepticism. While only 10% of executives believe employees do not know where to go when they need assistance on privacy matters, this skepticism doubles 20% among privacy team members. As it turns out, this view is closest to the reality of 18% of full-time employees either *disagreeing* or *strongly disagreeing* that they know exactly where to go when they need assistance with a privacy matter.

Overall, there was a general view among most respondents that their company views privacy and data protection as necessary. Indeed, almost half (45%) are strong advocates of their organization’s approach, believing that *privacy is of great importance and permeates every decision taken*.

Figure 5: **Importance of Privacy to the Organization**

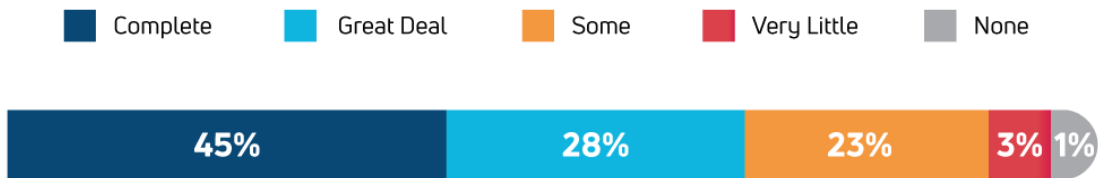


Perceptions of confidence

To get a sense of where confidence in organizations' ability to keep information secure and protected might be excelling or falling short, we asked respondents to weigh in on their perceptions of confidence in their own enterprise's ability to secure privacy for various stakeholders.

Although most respondents (73%) had high confidence in their company's privacy protection, this still leaves over a quarter of which were not.

Figure 6: **Overall Confidence in Company's Privacy Protection**

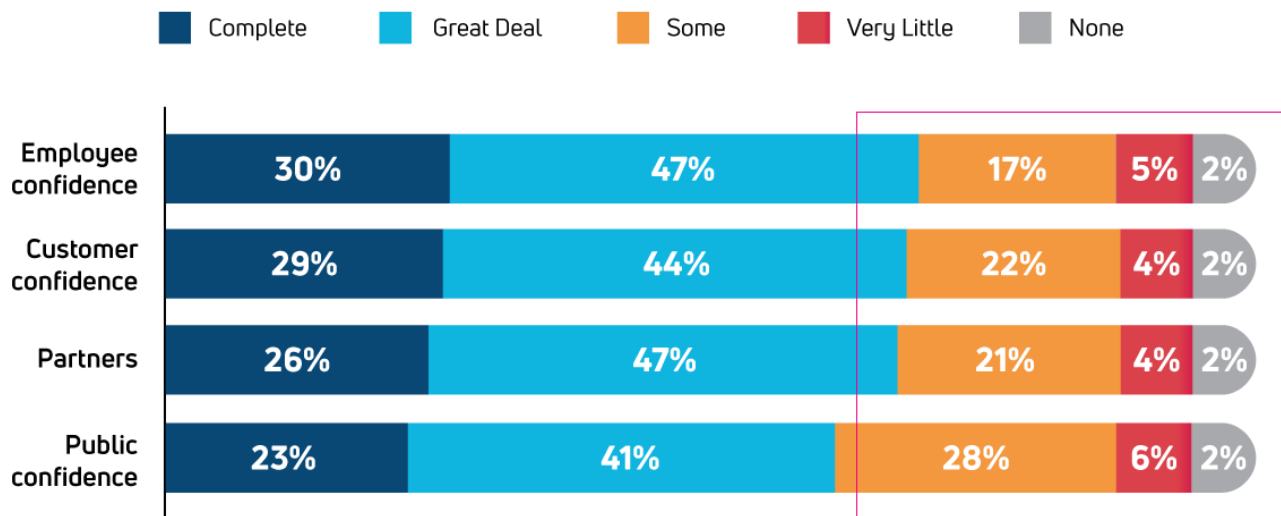


If someone asked you to keep a secret, would “probably” or “maybe” be an acceptable response?

Asked specifically about stakeholder groups, confidence was highest for employees and lowest in their belief of how the public viewed their company.

Disappointingly, and similar to the overall result, over a quarter felt only *some*, *very little* or *no* confidence in their company's ability to keep employee and customer data safe and protected. This lack of confidence was higher in Europe (30%) than in the United States (25%).

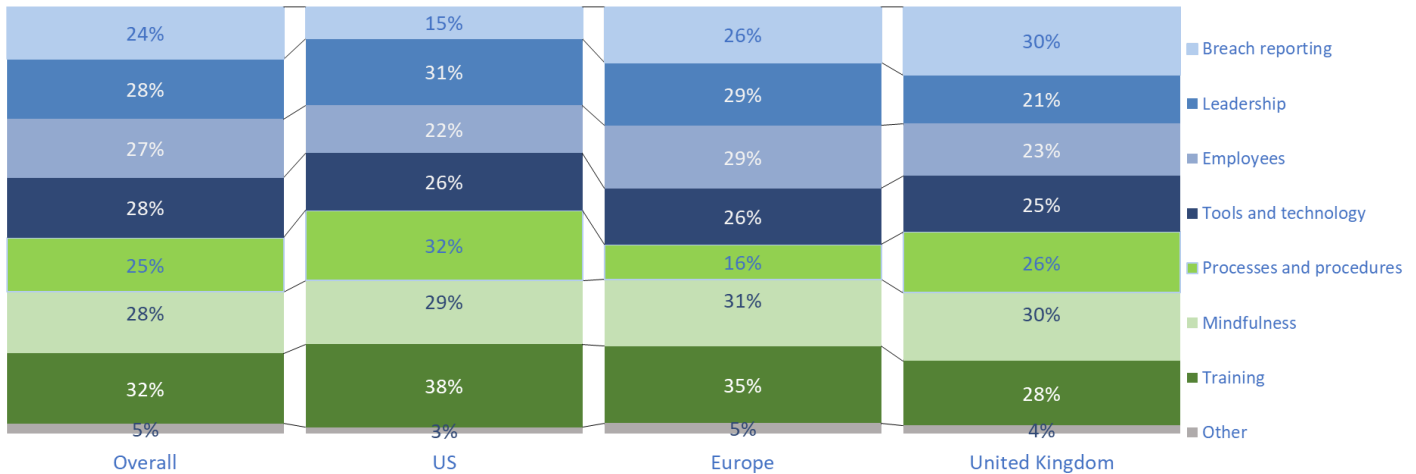
Figure 7: **Stakeholder Confidence in Privacy Protection**



When asked to reflect on why there may not be trust in the company's ability to keep information secure, respondents cited a lack of confidence that employees were adequately trained and aware of privacy needs (32%). Notably, respondents from exceptionally large companies were less likely to think employee training contributed to a lack of confidence. This difference may be due to having more capacity and resources for structured and deliberate training programs.

Among those who lacked confidence, we asked why and listed out various options.

Figure 8: **Areas Lacking Confidence***



*Note: A multi-pick all that apply option; therefore, figures do not add to 100%.

There were also significant variations by jurisdiction. Only 15% of respondents in the United States thought lack of confidence in data breach reporting and resolution was a key issue, compared to 26% in Europe and 30% in the United Kingdom. This is likely reflective of the breach laws in the US having been in place for a longer time than in the UK and Europe.

Again, we saw essential differences by role: 48% of privacy team members felt that low trust was attributable to a lack of confidence that all business functions are mindful of privacy requirements compared to only 26% of Senior Executives, Privacy Executives, and Management. Almost half of Management and Privacy Team members were also more likely to cite a lack of confidence in employee training and awareness (43% and 50%). In comparison, only about a quarter of Senior Executives (26%) and Privacy Executives (23%) viewed the problem this way.

The most challenging elements of privacy management

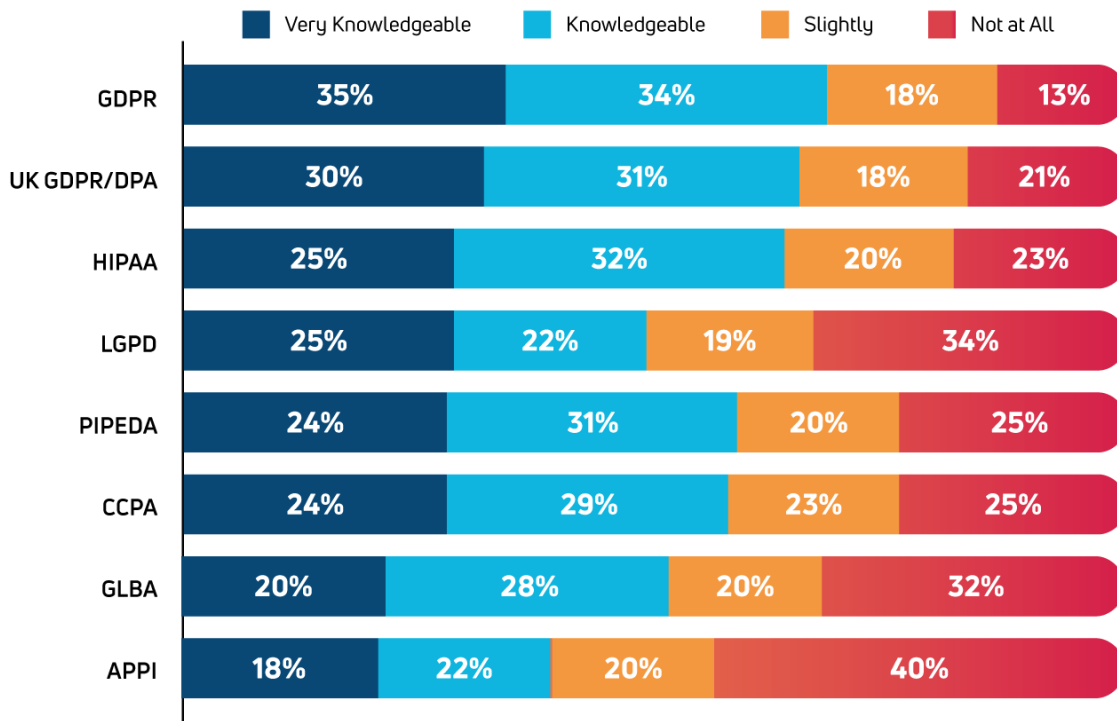
Asked which aspects of privacy management have been the most difficult, overwhelmingly respondents pointed to *staying current with privacy and security regulations* and *managing privacy risks* as the #1 and #2 challenges, respectively. Response variation by role followed an unsurprising pattern. While senior executives ranked staying current and managing risks the highest, privacy function executives were focused more on the “doing” of *data inventory/mapping*, *maintaining processing records*, and *privacy by design* issues.

Regulatory knowledge, impact, and compliance

Privacy stewardship requires a dedicated and concerted effort to understand what personal data an organization has, including its ownership, the applicable rights, and potential risks. Ultimately, it comes down to an organizational capacity to manage data. This capacity includes an understanding of applicable data subjects rights, the risks associated with organizational data, and the external obligations to remain “on side” with data regulations.

Many companies find themselves confronting a lack of knowledge about regulatory requirements, their reach, and what they mean in practice to comply. Knowledge of GDPR - the most comprehensive of all regulatory frameworks, was highest among respondents at 69%. While this is modest, among Privacy Executives, it was as expected substantially higher at 80%. Surprisingly, despite the looming July 1, 2020, CCPA compliance deadline, almost half (45%) of the respondents who will be required to comply with it claimed only *slight* or *no* knowledge at all of it.

Figure 9: **Self-Reported Regulation Knowledge***



Solutions and their effectiveness

Much of the compliance burden can be administrative. Privacy professionals have reported being the most bogged down by tasks like documentation, data mapping, and meeting turnaround times for regulatory reporting, noting that this leaves them with less time for things they want to be doing more of, such as internal training.²

As discovered previously, documentation and reporting should not be so challenging or time-consuming.³ New purpose-built software solutions with resource and time-saving automation, workflows, and trend analysis can help an organization identify and reduce known and emerging concerns before they have a negative impact on the company and its stakeholders.⁴ Other reports have found that the use of automation is increasing and is a common trait of effective data security and privacy programs.⁵

The right software makes it easier for organizations by:

² Nymity (now TrustArc). (2019, July). "Privacy Pulse." 1-9.

³ Ibid

⁴ NAVEX Global. (2019). "The Definitive Corporate Compliance Benchmark Report: Measure, Evaluate and Advance Your Program." 1-72.

⁵ Ibid

- reducing complexity while supporting privacy impact assessments, proactive risk notifications, and on-demand reporting,
- enabling quicker responses with automated solutions, for example, to fulfill data subject rights requests, and
- fostering a “culture of privacy” within the organization, offering relevant training, push notifications, and content.

Forrester’s 2020 assessment of privacy management software providers found that the key differentiators of leading privacy management software included formalized, automated processes, rich content, customizability of dashboards and workflows, and privacy risk assessments.⁶ Concurring with these viewpoints, we assessed stakeholder views of them worldwide.

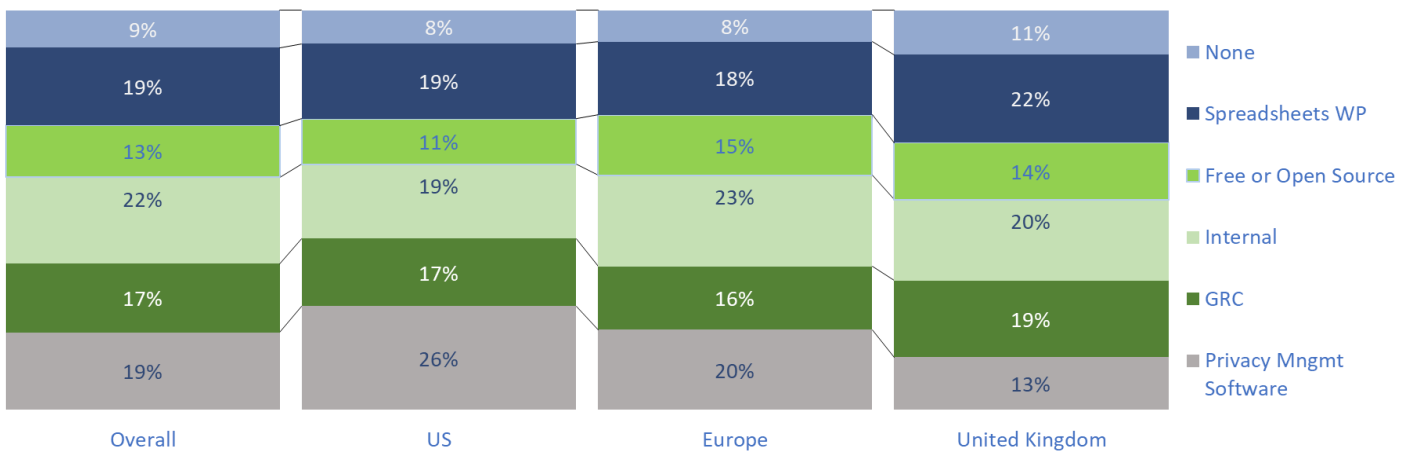
Among respondents, 23% are either not using any technology solution to implement privacy or are still using spreadsheets, email, and/or word processing software.

Despite stated commitments to the importance of privacy, a full quarter of respondents indicated that their companies do not have a robust tools approach. Only a third of respondents use purpose-built, automated software - either privacy management or GRC (governance, risk, and compliance) software. Some may find this finding surprising given that these software solutions have been in place for many years; others may not, as common barriers to technology adoption exist, including budget and comfort with technology. Notably, the use of purpose-built privacy management software is more prevalent in the United States (43%) than in Europe (36%) and the United Kingdom (32%).

Figure 10: **Primary Privacy Solution Software***

What primary solution do you use to manage your privacy program?

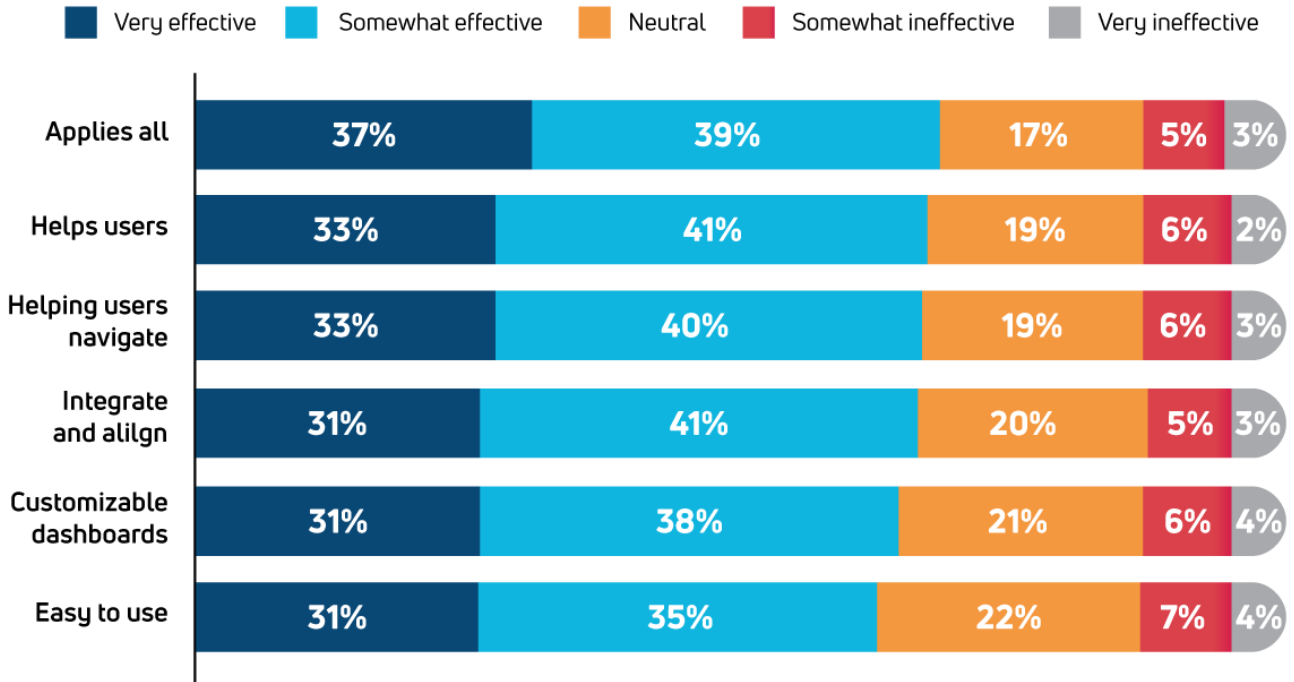
Excluding “Don’t Know” Responses



Despite the variance in solution adoption, most generally had respondents assessed their solution as *effective* or *very effective* on all fronts, from *applicability to all user groups* (e.g., privacy, legal, IT, marketing, sales, HR) to *ease of use*.

⁶ Iannopollo, E. (2020). “The Forrester Wave: Privacy Management Software, Q1 2020 The 15 Providers That Matter Most And How They Stack Up.” Forrester. 1-18.

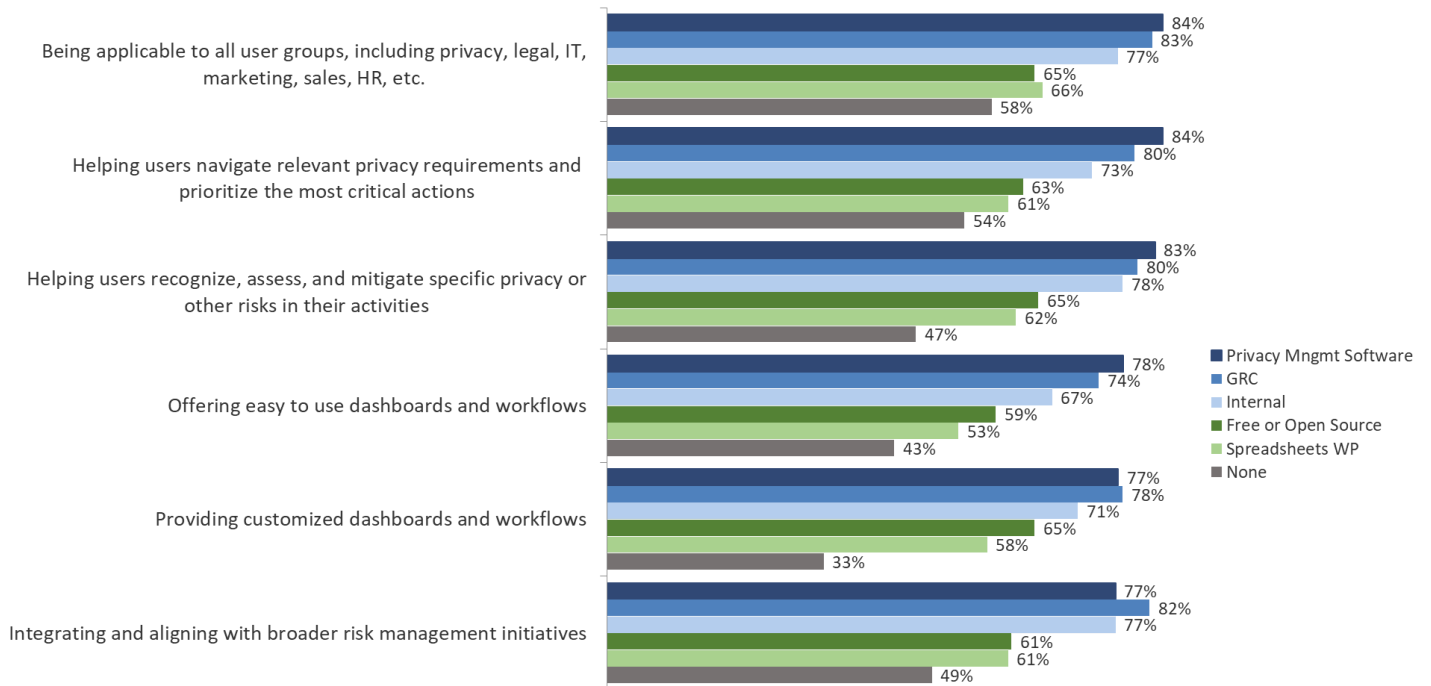
Figure 11: **Perceived Solution Effectiveness***



Notably, though purpose-built software had generally a 20 percentage point higher effectiveness rating than *free or open-source, spreadsheets/word processor* solutions, or indeed *no solution* in place.

Figure 12: **Solution Effectiveness for Each Solution Choice**

Solution Effectiveness (% Very + Somewhat) for each Solution Choice



Purpose-built, automated software sets apart companies with high levels of privacy confidence versus those without on all fronts.

For those who viewed their current solutions as lacking in meeting their needs, the following topped their list of deficiencies:

- automating processes,
- being easy to administer, and
- tracking how personal data is being processed for various purposes

Not surprisingly, the “doing” functions of software were rated most negatively by those charged with its execution. For example, while only 19% of senior executives were concerned with “how tracking personal data is being processed for various purposes,” 35% of privacy team members viewed it as coming up short with their software.

Budgeting for privacy

There is an enormous range that companies spend on privacy matters. An equal percentage (21%) annually spend \$50,000 or less, as do others who spend \$2,500,000 or more. For those readying for CCPA, a significant portion will be spent on these efforts.

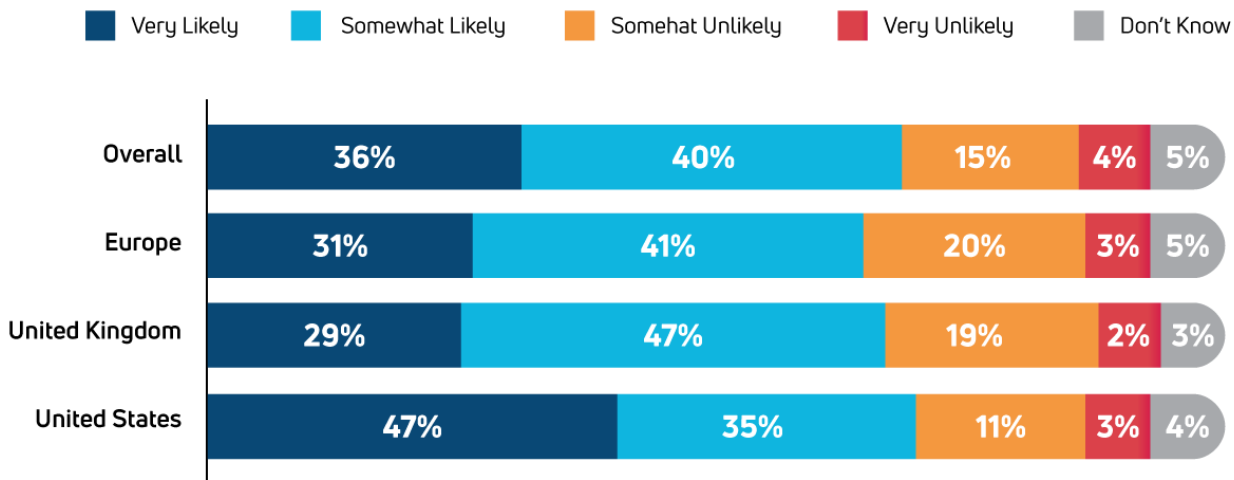
Approximately half (48%) had initially budgeted to pay more in 2020 than the previous year. At the same time, COVID-19 Pandemic put a dent in this spending; still, 41% are expected to maintain these increased budgets.

CCPA readiness

Although technically enforceable only for companies doing business in California, global companies operating with access to Californian’s data are required to maintain the CCPA principles. Not surprisingly then, when companies were surveyed before the deadline, some three-quarters (76%) believed they were very likely (36%) or somewhat likely (40%) to be ready for the July 1, 2020, required compliance date.

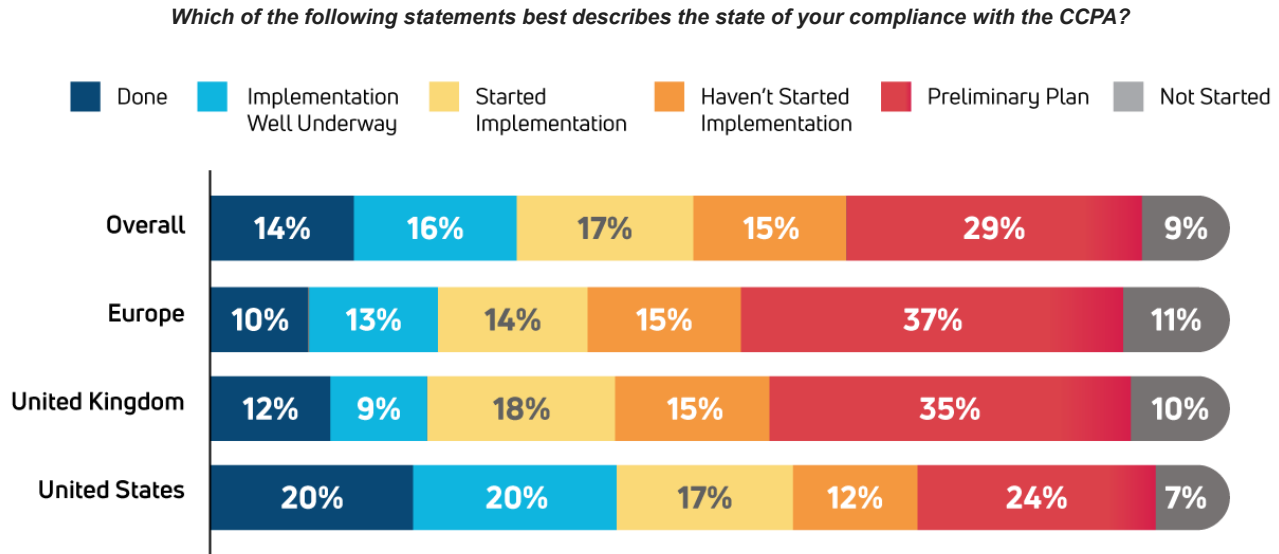
Figure 13: **Likelihood of CCPA Compliance**

How likely are you to be fully compliant with the CCPA requirements on the regulation enforcement date of July 1, 2020?



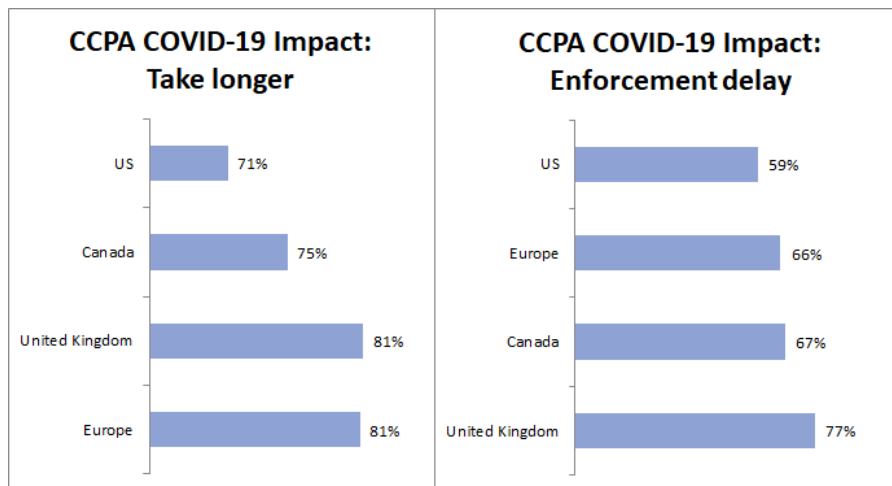
While US-based companies were slightly more bullish on their abilities, in stark contrast to this enthusiasm, still over half we surveyed in early May had either not started or were still only in the planning stages with CCPA. This finding arose despite less than 2 in 10 of those with knowledge of the regulations finding any of the elements challenging to achieve. Among US respondents, only 1 in 10 indicated it was difficult to achieve. These findings present somewhat contradictory opinions versus behaviors; being knowledgeable does not propel companies to comply.

Figure 14: **CCPA Compliance Preparedness***



Additionally, many “banked” on the Pandemic, causing a delay in CCPA regulatory enforcement despite what public officials had claimed. The vast majority of senior executives (85%) in particular believed it would cause delays. Further, companies with head offices outside the US were more likely to think (or hope) it will cause a delay.

Figure 15: **Covid-19 Perceived Impact on CCPA Compliance**



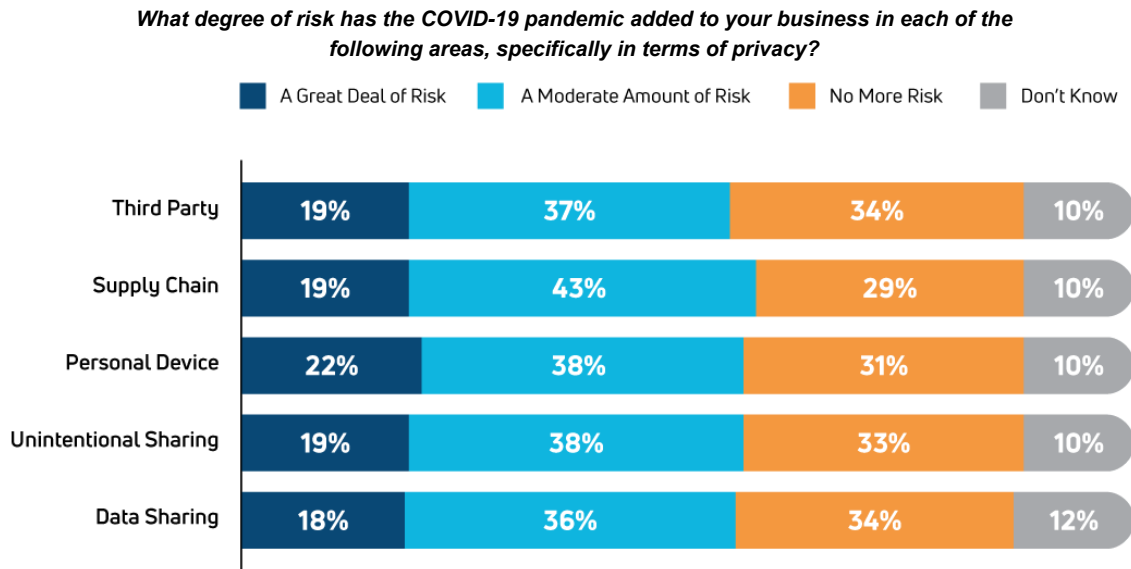
Pandemic impact on privacy

The fieldwork for this survey occurred during the first two weeks of May 2020. By that point, Covid-19 had forced a global response, including lockdowns in Europe, Asia, and North America. Some 42% of companies expected to suffer

either a *decrease* or *steep decrease* in revenues. When asked what percent of their company's workforce had switched to working from home due to COVID-19, 62% indicated that more than half their workforce had done so.

With these findings as context, we found across a variety of measures a 50%+ perceived increase in risk from the Pandemic, including third party risks and the risks from the use of personal devices.

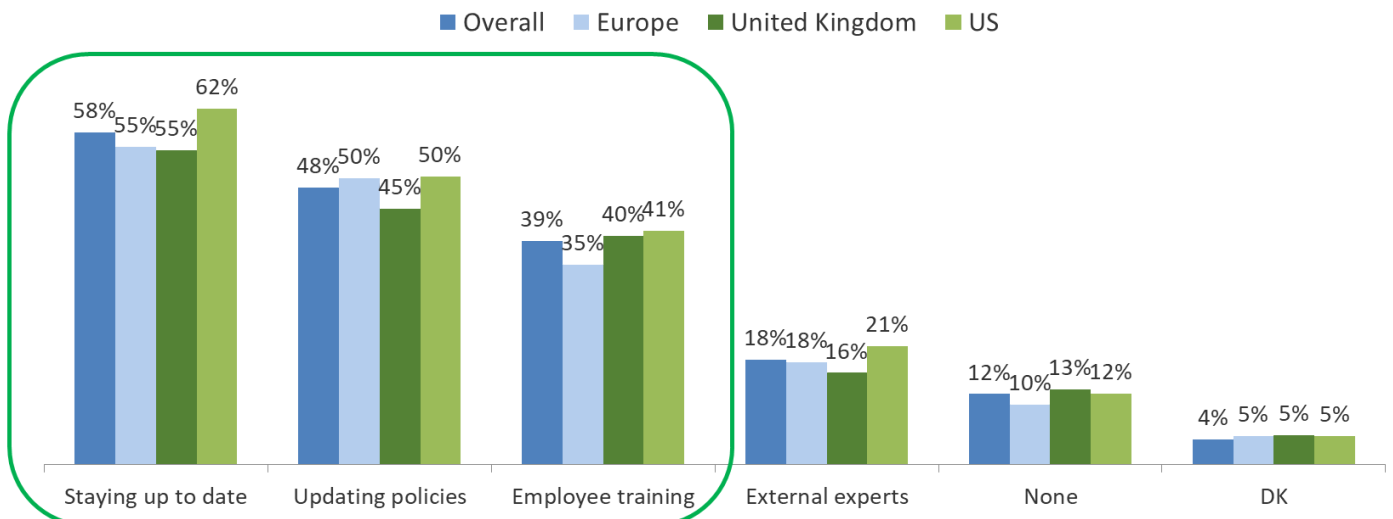
Figure 16: **Covid-19 Privacy Risks***



To tackle these risks, companies took additional measures: staying up to date on COVID-19 privacy concerns and regulations, updating policies accordingly, and training employees were the top initiatives. These findings held around the Globe.

Figure 17: **Taking Additional Measures as a Result of Covid-19***

As a result of COVID-19, are you taking any of the following measures?

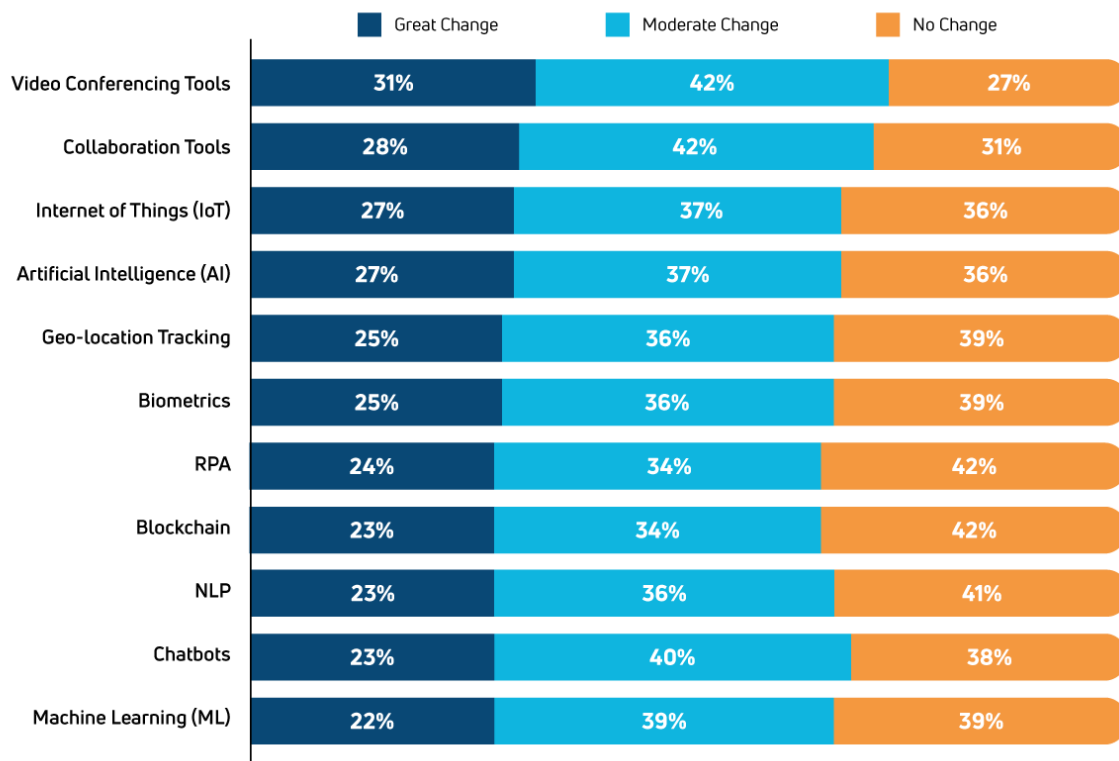


New technologies

The adoption of new digital technologies, from blockchain to AI, has impacted privacy rights. The Pandemic caused a rapid shift to remote working environments, exacerbating these privacy challenges, particularly with the accelerated use of video conferencing and collaboration tools.

Nonetheless, most claim to manage these new technologies because they were already underway in rethinking their approach, understanding the costs, and knowing the processes needed to ensure privacy. That is not to say significant efforts and expenses should be downplayed. Several new technology requirements pose cost and effort challenges. For instance, complying with the right not to be processed in a fully automated process can increase the cost and limit the application scope of machine learning and AI to process and make sense of large quantities of data.^{7, 8} Similarly, compliance with the “right to delete” principle can complicate blockchain applications, whereas the requirement to obtain active consent for all intended data uses could impact the use of cloud computing technologies.⁹

Figure 18: **Digital Technology Impact on Privacy**



On the other hand, these technologies can also enable compliance and help companies manage cost and resource requirements. For example, AI can identify, prepare, clean, delete and mask personal information. As call centers increasingly shift to interfaces like chatbots and automated Natural Language Processing (NLP) voices, AI can also help detect when personal data is being shared. Then, AI can mask, block or delete it so that the organization is not exposed to compliance risk. Interestingly, our findings on the privacy impact of AI causing a *great deal of change* were

⁷ McKinsey & Company. (2018, July 31). “Data privacy: What every manager needs to know.” [Transcript].

⁸ Li, H., Yu, L., & He, W. (2019). The Impact of GDPR on Global Technology Development. *Journal of Global Information Technology Management*, 22(1), 1-6.

⁹ Ibid

felt differently across organizational levels: more by senior executives (30%) than management (22%) or full-time employees outside the privacy function (8%).

Companies that get ahead of these requirements by leveraging innovative technologies and automation can create a solid economic moat and resilience versus companies who ignore them and soon find themselves offside with regulators, their customers, and potentially the public at large.

Conclusion

Hearts, minds, and actions

-- across the globe, in all industries, and at all organizational levels --

people generally have their hearts in the right place when it comes to the importance of privacy. Still, many have only limited knowledge about the regulations impacting their business, and many more again have been slow in adopting new regulatory requirements.

COVID-19 created unexpected challenges when there was already increased pressure on data and privacy protection measures for companies as a result of the adoption of CCPA. Many companies stepped up to the challenge while others fell behind – overwhelmed by the new looming requirements combined with pandemic imposed difficulties such as work from home and personal device use, despite potentially disastrous implications such as the unintentional sharing of customer and employee data.

Companies with purpose-built, professional privacy software and solutions fared markedly better than others in their global privacy commitments, approaches, and outcomes. The right privacy tools made it easier for organizations to tackle complexity and *unprecedented change*, the new catchphrase that summarized 2020.

Along with embracing new technologies, forward-thinking companies seized privacy as a strategic opportunity to gain a competitive edge. Rethinking “business as usual,” some leaped ahead of the curve by instrumenting a comprehensive and coordinated approach to privacy that went beyond a regulatory compliance exercise. While others stumbled, they led with a privacy culture that permeated their entire organization and differentiated them in the marketplace.

About TrustArc

As the leader in data privacy, TrustArc automates and simplifies creating end-to-end privacy management programs for global organizations. TrustArc is the only company to deliver the depth of privacy intelligence, coupled with the complete platform automation essential for the growing number of privacy regulations in an ever-changing digital world. Headquartered in San Francisco and backed by a global team across the Americas, Europe, and Asia, TrustArc helps customers worldwide demonstrate compliance, minimize risk, and build trust. For additional information, visit www.trustarc.com.

About Golfdale Consulting

Golfdale Consulting Inc., trusted advisors to growth-focused business leaders. Golfdale expertise spans three critical areas: global market research and insights, analytics strategies and application of decision sciences, and advocacy for evidence-based regulatory reform and market impact.