CORPORATE DATA PRIVACY TODAY:
A LOOK AT THE CURRENT STATE OF READINESS, PERCEPTION AND COMPLIANCE
Data privacy and data protection have become some of most significant and talked-about business issues in modern society.

Rooted in heavyweight, globally-reaching regulations including the General Data Protection Act (GDPR) and the California Consumer Privacy Act (CCPA), a new era has emerged, bringing the “wild wild west” of data management to an end. At the same time, data is gaining momentum as an increasingly valuable business asset.

At the GDPR’s one-year anniversary, enforcement actions resulted in €56,000,000 in fines, and as of January 2020, total fines have risen to €114,000,000. Hundreds of cases are currently under review with European data privacy authorities. When the CCPA came into effect in 2020, experts estimated compliance to cost an initial $55 billion for businesses ranging from small, independent companies to large corporations. Additional U.S. state and federal laws surrounding data privacy are sweeping across dozens of legislative sessions. More regulations are expected to emerge worldwide.

To better understand how organizations are limiting their use of consumer data, and balancing the costs and risks of managing data in compliance with privacy laws, FTI Consulting recently surveyed more than 500 leaders of large, U.S.-based companies. All of the respondents—60 percent held titles in senior management or the C-suite and 28 percent held middle-management roles—had knowledge of their organizations’ data privacy policies and activities. The results provided a robust illustration of the state of data privacy today, and the data privacy programs, perceptions and strategies at large corporations. This is part one of two reports examining the survey’s findings.

A number of key themes—some insightful, some surprising, some aligned with what our experts are seeing among clients—came to light in the responses. These insights will provide legal, compliance, IT and privacy teams with a way to benchmark their own initiatives against what’s taking place across the big picture:

- **Change Is the Only Constant**
- **Organizations Face Pervasive Risk**
- **Awareness Does Not Always Lead to Prioritization**
- **People, Process and Technology are Needed**

### CHANGE IS THE ONLY CONSTANT

In response to global data privacy regulatory pressure, **75 percent of organizations surveyed have made changes in the last 12 months.** Most plan to keep doing so in the coming year and beyond. Nearly all respondents plan to increase their data privacy spend, many by 50 percent. Yet regulatory uncertainty is a major concern, and one that will drive continued change for the foreseeable future.

*Has your organization changed its data privacy compliance in response to regulatory pressure over the last 12 months?*

<table>
<thead>
<tr>
<th></th>
<th>Overall</th>
<th>Manufacturing</th>
<th>Tech Services</th>
<th>Financial Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes, and we will continue to adapt</td>
<td>87%</td>
<td>83%</td>
<td>87%</td>
<td>83%</td>
</tr>
<tr>
<td>Yes, but we won’t adapt any further</td>
<td>16%</td>
<td>16%</td>
<td>7%</td>
<td>5%</td>
</tr>
<tr>
<td>No, but we intend to over the next 12 months</td>
<td>7%</td>
<td>4%</td>
<td>4%</td>
<td>5%</td>
</tr>
<tr>
<td>No, and we don’t intend to</td>
<td>5%</td>
<td>5%</td>
<td>5%</td>
<td>2%</td>
</tr>
<tr>
<td></td>
<td>3%</td>
<td>2%</td>
<td>2%</td>
<td>2%</td>
</tr>
</tbody>
</table>

“Normally, this level of budget increase is virtually unheard of, especially in an area long viewed as providing nominal business value. The fact that nearly all of the survey respondents plan to increase data privacy budgets, and most by a significant margin, indicates a major shift in thinking. We’re now seeing data privacy enablement viewed not as a pesky cost of doing business, but as a critical practice that can mitigate risk and create tremendous value,” said Jake Frazier, Senior Managing Director, FTI Technology.

### Regulatory Unease

The biggest challenge for data privacy over the next 12 months was deemed by respondents as “regulatory inconsistencies across markets”.

---

FTI Consulting, Inc.
BUDGETS ON THE RISE:
97% will increase data privacy budgets this year, with an average increase of 50%.

Perception vs. Reality
The survey revealed disparity between identified concerns and public perceptions. One example is the issue of data subject access requests (DSARs), which are often in the spotlight as a significant challenge of data privacy compliance. The survey showed that DSARs actually ranked lower on the list of concerns.

Which of the following aspects of data privacy are you particularly concerned about?

<table>
<thead>
<tr>
<th>Aspect</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber breaches</td>
<td>44%</td>
</tr>
<tr>
<td>Data usage, limitations of usage, and sharing data with third parties</td>
<td>42%</td>
</tr>
<tr>
<td>Employee hardware loss (laptop, thumb drive, company phone)</td>
<td>39%</td>
</tr>
<tr>
<td>Regulatory investigations, sanctions, potential disputes and litigation</td>
<td>37%</td>
</tr>
<tr>
<td>Internal data theft</td>
<td>37%</td>
</tr>
<tr>
<td>Impact on my organization’s reputation</td>
<td>34%</td>
</tr>
<tr>
<td>Responding to Data Subject Rights</td>
<td>27%</td>
</tr>
<tr>
<td>Nothing</td>
<td>5%</td>
</tr>
</tbody>
</table>

“...the gaps between what the media and technology vendors are focused on, versus what issues are top of mind for corporations. With regard to DSARs, it could be that privacy teams have not yet experienced the full extent of the burden, or that other risk factors and privacy-related costs simply outweigh those of responding to DSARs. Either way, I think 2020 will be a pivotal year in terms of expectation setting and solidifying best practices around DSRs and other data privacy challenges,” said Chris Zohlen, Managing Director, FTI Technology.

No Magic 8 Ball
Respondents are also concerned about a number of uncertainties in the current landscape. “Regulatory change in my country” was a concern for 38 percent and “political uncertainty” was a concern for 34 percent.

ORGANIZATIONS FACE PERVERSIVE RISK
One of the most glaring findings in the survey was the expectation for a nine percent drop in global annual turnover as a result of a data privacy crisis event. Respondents explained this drop would manifest through “very negative” impacts on organizational reputation, investor confidence, business operations and external relationships. Based upon the respondent organizations’ current average annual turnover cost of $830 million, these effects are estimated to cost $79 million in losses.

Pressure Takes Many Forms
Between 23 percent and 40 percent of organizations feel data privacy compliance pressure from a variety of sources, including the board, the media, customers, competitors regulators and more. Three quarters cited “government and regulators” as a source of extreme or significant pressure.

Scrutiny Runs High
Sixty percent agree or strongly agree that their organization is under more scrutiny due to an increased awareness or expectation around how data is managed.

This is borne from specific data privacy regulations, with 20 percent impacted but not fully compliant with GDPR, and 28 percent affected by, but under-prepared for, the CCPA.

60% agree; organizations are under more scrutiny due to increased expectations around how data is managed.
How have the following data privacy regulations impacted your organization?

<table>
<thead>
<tr>
<th>Regulation</th>
<th>Impacts, but we aren’t fully compliant</th>
<th>Impacts, but we are compliant</th>
</tr>
</thead>
<tbody>
<tr>
<td>GDPR</td>
<td>19%</td>
<td>16%</td>
</tr>
<tr>
<td>CCPA</td>
<td>8%</td>
<td>7%</td>
</tr>
<tr>
<td>FTC</td>
<td>4%</td>
<td>4%</td>
</tr>
<tr>
<td>HIPAA</td>
<td>13%</td>
<td>12%</td>
</tr>
<tr>
<td>LGPD</td>
<td>23%</td>
<td>21%</td>
</tr>
<tr>
<td>GLBA</td>
<td>36%</td>
<td>34%</td>
</tr>
</tbody>
</table>

- I’m not aware of this
- Does not impact and we do not expect it to in the near future
- Does not impact, but we expect it to in the next 12 months

### Global Privacy in Force

It’s no surprise that organizations feel intense pressure from data privacy authorities. Worldwide, privacy law includes:

**Europe:**
- GDPR
- ePrivacy Regulation, anti-spam, healthcare, cloud computing

**North America:**
- California Consumer Privacy Act
- Digital Privacy Act
- HIPAA/HITECH
- New York State Department of Financial Services Cyber Security Regulation
- Personal Information Protection and Electronic Documents Act (PIPEDA)

**Latin America:**
- General Data Protection Law (LGPD)
- Organization of American States/Inter-American Committee Against Terrorism (OAS/CICTE)
- Cybersecurity Protection, cross-border data transfer restrictions, healthcare, data breach and cloud computing

**Asia Pacific:**
- China’s Cybersecurity Law
- China’s State Secrets Law
- Japan Act on the Protection of Personal Information, healthcare privacy, cloud computing, marketing activities

### Serious Side Effects

Most organizations (75 percent) expect that a data privacy crisis would result in negative impacts across a range of areas. More than 30 percent said the impact to relationships and organizational reputation would be “very negative.” Moreover, 37 percent are “particularly concerned” about “regulatory investigations, sanctions, potential disputes and litigation,” regarding data privacy.

*In the event of a data privacy crisis, how much of a negative impact do you consider this will have on the following?*
“Consumers are going to be more aware of how their data is being used and increasingly ready to exercise the new rights and controls they have over it. Consumer concerns around privacy are on the rise. This will lead to an increase in DSARs, right of action claims and other activity related to consumer privacy rights,” said Deana Uhl, Senior Director, FTI Technology.

Riskiest Areas

Data usage, limitations of usage and sharing with third parties stood out as one of the highest ranked areas of risk in data privacy. Breaches, internal data theft, employee hardware loss and regulatory investigations and sanctions also ranked as leading concerns.

AWARENESS DOESN’T ALWAYS LEAD TO PRIORITIZATION

The survey confirmed that board members and corporate leaders are knowledgeable of and committed to data privacy compliance. While 81 percent said their executives understand the issues, awareness isn’t translating to a prioritization of data privacy at more one-third of organizations surveyed. At the same time, many organizations have a positive self-assessment of their privacy compliance, suggesting inconsistencies between awareness, prioritization, perception and readiness.

Underprepared and Vulnerable

Seventy-nine percent of respondents feel vulnerable to a data privacy crisis, and nearly 40 percent claim to be very vulnerable. When looking at specific industry segments, the number that feel very vulnerable jumps to 48 percent for technology services organizations and 43 percent for financial services institutions. Among all respondents, 61 percent say they are fully prepared for such a crisis and five percent say they are wholly unprepared.

79% of respondents feel vulnerable to a data privacy crisis, and nearly 40% claim to be very vulnerable.
How prepared or unprepared is your organization to deal with a data privacy crisis event?

- Unprepared
- Partly prepared
- Fully prepared

Overall: 61% Unprepared, 33% Partly prepared, 6% Fully prepared
Manufacturing: 61% Unprepared, 34% Partly prepared, 5% Fully prepared
Tech Services: 77% Unprepared, 22% Partly prepared, 1% Fully prepared
Financial Services: 67% Unprepared, 25% Partly prepared, 8% Fully prepared

Inconsistent Responses Suggest Confusion
Despite a majority of respondents citing a positive data privacy compliance self-assessment, feelings of vulnerability to exposure or enforcement run high.

“This suggests respondents may have inflated self-assessments, lack of understanding about the realities of data privacy regulations or unwarranted fear about the extent of their risk,” Zohlen said.

Moderate In-House Support
Overall, 57 percent of organizations surveyed have appointed in-house staff dedicated to data privacy compliance and crisis response.

Not All Industries Are Created Equal
Certain industries (such as those in financial services or retail) are at higher risk due to the high volume of sensitive, personal information they process and store in the course of everyday business. The differences in data privacy worry and practice within these industries were evident in the survey. It found that technology and financial services are more likely to have in-house teams to respond to a data privacy crisis event. Leaders in technology and financial services were also notably more knowledgeable and committed to data privacy when compared to manufacturing.

PEOPLE, PROCESS AND TECHNOLOGY ARE NEEDED
Like any business-critical issue, data privacy compliance cannot be solved by any singular method. Successful data privacy risk mitigation involves a healthy mix of people, process and technology. The survey revealed a strong technology position among most respondents, but gaps in internal expertise and process.

Technology Stands Out
Most respondents (68 percent) rated systems and technology as very effective for data privacy compliance. Implementing new programs and specific data privacy training were rated as very effective by 57 percent.

Internal Diligence: Room for Improvement
At 58 percent of organizations, new products are vetted for their impact to data privacy from the beginning. This leaves more than 40 percent not building privacy into the design of products and systems, instead waiting until a later stage in the process (25 percent), or until the end of implementation, or after a problem arises (16 percent).

At which point in the life cycle of a new product does it get reviewed for data privacy concerns?

“IT'S ENCOURAGING TO SEE MANY CORPORATIONS VETTING THEIR SYSTEMS FOR DATA PRIVACY COMPLIANCE AT THE OUTSET. BUT ALMOST HALF ARE WAITING TOO LONG TO DO THIS IMPORTANT EVALUATION. INVOLVING LEGAL AND COMPLIANCE TEAMS EARLY ON IN THE SOFTWARE SELECTION PROCESS IS KEY TO REDUCING THE TIME, COST AND RISK OF ONBOARDING NEW SOLUTIONS,” SAID ANDREW SHAXTED, SENIOR DIRECTOR, FTI TECHNOLOGY.
Lack of Resources

Nearly 60 of respondents agreed with the statement: “We don’t have the resource in our organization to ensure that we are fully compliant with data privacy regulation.”

How strongly do you agree or disagree with the following statements: “We don’t have the resource in our organization to ensure that we are fully compliant with data privacy regulation?”

<table>
<thead>
<tr>
<th></th>
<th>Strongly disagree</th>
<th>Slightly disagree</th>
<th>Slightly agree</th>
<th>Strongly agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall</td>
<td>21%</td>
<td>23%</td>
<td>13%</td>
<td>20%</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>22%</td>
<td>32%</td>
<td>28%</td>
<td>18%</td>
</tr>
<tr>
<td>Tech Services</td>
<td>28%</td>
<td>23%</td>
<td>42%</td>
<td>32%</td>
</tr>
<tr>
<td>Financial Services</td>
<td>29%</td>
<td>21%</td>
<td>42%</td>
<td>30%</td>
</tr>
</tbody>
</table>

“With the California Consumer Privacy Act coming into force, organizations are going to feel the pinch for resources needed to comply. This will include large companies spending in the range of $1-2 million on establishing and maintaining compliance,” Frazier said.

CONCLUSION

The survey findings indicate that data privacy will continue to keep legal, compliance, infosec and business executives up at night. New and emerging laws and ramping enforcement are driving corporations to audit existing practices, revise processes, add staff and massively increase privacy budgets. While progress is moving in the right direction, there is more work to be done. Organizations will need to translate their awareness to more action and diligence. As this happens, and privacy postures strengthen, organizations will begin to uncover and focus on the opportunities surrounding their data—rather than the risk.

When data is better understood, better catalogued, better managed, etc., it can ultimately be better leveraged as a valuable business asset. Organizations that have adequately addressed their risk—and in parallel approach data privacy compliance with an opportunistic mindset—will be strongly positioned for the new decade.

Nearly 60% do not have the resources to ensure full compliance with data privacy regulation.
METHODOLOGY

This survey was conducted by FTI Consulting during November 2019. More than 500 leaders of large-sized private sector companies, based in the U.S., with knowledge of data privacy policies and strategies, were polled. The profile of the respondents includes the following:

**Where in the US are you mainly based for work?**

- South Atlantic: 24%
- Mid-Atlantic: 18%
- East North Central: 14%
- Pacific: 14%
- West South Central: 14%
- New England: 8%
- Mountain: 6%
- West North Central: 5%
- South Central: 4%
- East South Central: 7%
- South Atlantic: 24%

**What industry does your company mainly work in?**

- Privately owned: 35%
- Publicly listed: 65%

**Which of the following best describes your position in your organization?**

- C-suite: 23%
- Middle management: 37%
- Senior management: 12%
- Lower management: 28%

**How involved are you in data protection, privacy, compliance and regulation for your organization?**

- Fully involved: 70%
- Partly involved: 19%
- Not involved, but knowledgeable: 11%

**By Industry:***

- **Overall**
  - Fully involved: 70%
  - Partly involved: 19%
  - Not involved, but knowledgeable: 11%

- **Manufacturing**
  - Fully involved: 73%
  - Partly involved: 13%
  - Not involved, but knowledgeable: 7%

- **Tech Services**
  - Fully involved: 89%
  - Partly involved: 8%
  - Not involved, but knowledgeable: 3%

- **Financial Services**
  - Fully involved: 72%
  - Partly involved: 22%
  - Not involved, but knowledgeable: 7%
Which of the following would you use to describe your organization?

- Technology Services: 24.1%
- Other: 11.9%
- Financial Services: 11.1%
- Manufacturing: 10.4%
- Healthcare and Social Work: 8.7%
- Professional Scientific and Technical Activities: 4.5%
- Agriculture, Forestry, and Fishing: 4.5%
- Wholesale and Retail Trade: Repair of Motor Vehicles and Motorcycles: 4.3%
- Construction: 3.5%
- Accommodation and Restaurant Services: 3%
- Real Estate Services: 2.6%
- Arts Sports Entertainment and Recreation and Other Activities: 2.4%
- Transport and Storage: 2.2%
- Mining and Quarrying: 2%
- Education: 1.5%
- Supply of Electricity, Gas, Steam and Conditioned Air: 1.5%
- Water Supply: Sewage Systems, Waste Management and Sanitation: 1.3%
- Renting Services Travel Agencies Business Support Services: 1.6%

Approximately, what is your global turnover?

- Mean = USD$870M

Approximately how many data subjects (individuals) does your organization hold?

- Mean = 73,000

About FTI Consulting

FTI Consulting is an independent global business advisory firm dedicated to helping organizations manage change, mitigate risk and resolve disputes: financial, legal, operational, political & regulatory, reputational and transactional. FTI Consulting professionals, located in all major business centers throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges and opportunities. For more information, visit www.fticonsulting.com and connect with us on Twitter (@FTIConsulting), Facebook and LinkedIn. FTI Consulting, Inc., including its subsidiaries and affiliates, is a consulting firm and is not a certified public accounting firm or a law firm.

The views expressed herein are those of the author(s) and not necessarily the views of FTI Consulting, Inc., its management, its subsidiaries, its affiliates, or its other professionals.

www.fticonsulting.com

©2020 FTI Consulting, Inc. All rights reserved.