Getting to GDPR Compliance: Risk Evaluation and Strategies for Mitigation

Executive Summary

The European Union's General Data Protection Regulation presents compliance challenges for organizations across industries and geographies. American firms struggle with the law's complexity. Even among European firms, which presumably have already built data protection programs to comply with the EU Data Protection Directive, the GDPR requires new investments in privacy resources.

The risks of not complying, of course, include fines up to 4 percent of global turnover. But not all non-compliance is created equal and – given the law's implementation deadline of May 25, 2018 – privacy professionals must prioritize.

To gauge the risks of non-compliance with various aspects of the GPDR, the IAPP surveyed nearly 500 privacy pros, most of whom work for organizations headquartered in either the United States (44 percent) or the European Union (including the United Kingdom, 44 percent). We asked them to rate the risk of non-compliance with various requirements of the GDPR and what actions they are taking to mitigate each perceived GDPR risk.

What was the number one action item to mitigate GDPR compliance risk? Investment in training. Training employees on data protection and privacy tops the list for 10 of 11 GDPR compliance risks. The only risk training doesn't mitigate is appointing a data protection officer, which obviously requires taking other steps.

The second most likely response to GDPR risks is investments in technology. These results conform precisely to the 2017 IAPP-EY Privacy Governance Report, which similarly found that investments in training and technology are the top two GDPR-preparedness activities.

Regarding the risks themselves, respondents overall rate failing to prepare for data breach notification as the highest GDPR compliance risk, with failure to conduct data inventory and mapping coming in a close second. Not obtaining data subject consent and improperly handling international data transfers tie for third place overall. Among U.S. respondents, however, not complying with requirements around international data transfers ranks as the top GDPR risk – and earns the highest overall risk score.

Training employees on data protection and privacy tops the list for 10 of 11 GDPR compliance risks.

Although they are struggling with GDPR's complexity, American respondents are still bullish on their ability to be ready by the May 25 deadline. Indeed, 84 percent of U.S. respondents expect to be GDPR-compliant by May 25, 2018.

EU privacy professionals are either less concerned or more honest – or perhaps lacking in resources – because more than one in four say they will not be ready on time. Their biggest barrier, they say, is lack of adequate budget.

Background and Methodology

In September and October 2017, the IAPP fielded a survey to subscribers to the IAPP Daily Dashboard. The survey asked respondents to identify their organization's headquarters and industry, and whether they believe the GDPR will apply to their employer's operations. Those who answered "no" did not continue with the survey.

The survey asked the remaining participants – 88 percent of the total – to answer a series of questions scoring the risk of failure to comply with certain obligations under the GDPR, with 1 being "no risk," 2 "low risk," 3 "moderate risk," 4 "elevated risk," and 5 "high risk." The GDPR compliance obligations we queried about were:

- Operationalizing the right to be forgotten.
- Operationalizing data portability.
- Obtaining/managing user consent.
- Complying with international data transfer requirements.
- Preparing for data breach notification.
- Conducting data protection impact assessments.
- Establishing legitimate interest for data processing.
- Conducting data inventory/mapping.
- Maintaining records of processing (e.g. Article 30 reports).
- Managing data subject requests.
- Appointing a data protection officer (DPO).

For each of the 11 failure-to-comply risks, the survey asked respondents to identify the steps they are taking to mitigate that risk, choosing as many as they'd like among six options:

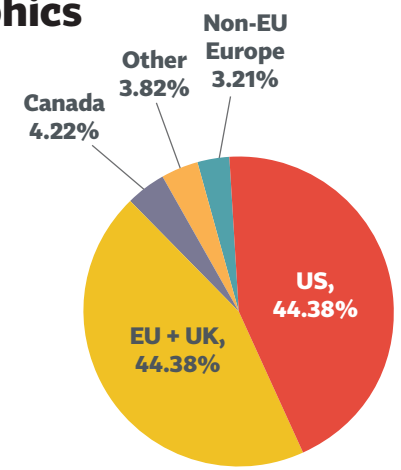
- Investing in privacy/data protection training.
- Increasing number of privacy staff.
- Investing in additional outside legal assistance.
- Investing in additional outside consulting assistance.
- Investing in privacy/data protection technology.
- Or continuing the status quo privacy program.

Next, we asked respondents to demonstrate how far along they are in complying with the GDPR, on a sliding scale from 0 to 100 percent, and when they expect to be fully compliant.
Finally, we asked what barriers they face to achieving GDPR compliance, choosing among the following:

- Inadequate budget.
- Lack of qualified privacy staff.
- Too little time.
- Complexity of the law.
- And shortage of technical tools.

Respondent demographics

We received a total of 498 responses, 44 percent of which were from respondents headquartered in the U.S. and 44 percent of which were from respondents headquartered in either the U.K. or elsewhere in the EU. A statistically insignificant number responded from Canada, European countries not in the EU, and elsewhere.



Three quarters of respondents were from companies with fewer than 25,000 employees, but the survey reflects a balanced distribution from privacy professionals working in firms of varying size.

Company Size

Number of employees	% respondents
< 100	12.25%
100-999	22.49%
1,000-4,999	20.48%
5,000-24,999	20.68%
25,000-74,000	10.24%
75,000 +	13.86%

GDPR Compliance Risks and Responses

Among respondents, 88 percent report their organization falls under the scope of the GDPR, while 12 percent believe it does not. This number is slightly different – but within the margin of error – from the 95 percent reporting GDPR applies to them in the 2017 IAPP-EY Privacy Governance Report. Among those who answered "no" to whether the GDPR applies to their organization, a majority are from the U.S. (55 percent), and one in four works in the government sector.

In any legal compliance situation, it can be difficult to know in advance what will trigger a regulator's investigation or enforcement action. Typically, regulators discover non-compliance with privacy law due to an incident such as a data breach,

Does Your Organization Fall Under the GDPR?

	U.S.	EU
Yes	85%	98%
No	15%	2%

	Number of Employees		
	< 1,000	**1,000-24,999**	**>25,000**
Yes	86%	88%	**92%**
No	14%	12%	8%

whether reported by the organization suffering the breach or by someone else. It's not surprising, then, that respondents overall cited failure to be prepared to provide prompt data breach notification under GDPR Articles 33 and 34 as presenting the greatest non-compliance risk (see full chart, page 5), and that risk was the top one for EU respondents as well.

Further, the slippery nature of data, easy to quickly distribute and held in many places throughout an organization, makes data inventory and mapping a tall task. No wonder, then, that accounting for the what and where of personal data comes in second on the list of non-compliance risks among all respondents and among EU respondents.

Failing to track data subject consent is also highly risky, and it earned the third highest compliance-risk scores for all respondents. Organizations that get it right can use consent as the basis for many data processing activities, including cross-border data transfers. But organizations that get it wrong

risk upsetting data subjects, who may file complaints with the local data protection authority and go elsewhere with their business.

However, priorities and risk evaluations are not always the same on differing sides of the Atlantic Ocean.

It's no surprise, perhaps, that when we drill down into what concerns organizations in the U.S., we find they lose the most sleep over transferring data outside of the EU, ranking failing to get data transfer compliance right as the most risky. Because so many of them will rely on consent as a lawful basis for processing and transfer, moreover, obtaining proper consent ranks second on their list of compliance risks.

Somewhat surprising are the lower compliance-risk scores assigned, across the board, to "establishing legitimate interest" as a lawful basis for data processing and international data transfer; complying with data portability obligations; and appointing a data protection officer. These are either perceived as easy compliance responsibilities that require only a light lift, something that data protection authorities or data subjects will not prioritize, or actions already underway so that non-compliance is unlikely.

Certainly in the case of appointing a DPO – where 24 percent of respondents rated it a "1" for "no risk" – it's likely this is something most organizations who must comply with the GDPR have already done, and have thus checked it off the list of concerns. Indeed, when asked what they are doing to mitigate the

How Risky Is Non-Compliance With the Following GDPR Obligations
(Scale Of 1-5, With 1 Being "No Risk" And 5 Being "High Risk")

Overall		U.S.		EU	
Prep. for breach	3.66	Int'l data transfers	3.76	Prep. for breach	3.68
Data inventory/mapping	3.57	Obtaining consent	3.61	Data inventory/mapping	3.57
Obtaining consent	3.54	Prep. for breach	3.6	Maintain. Art. 30 records	3.51
Int'l data transfers	3.54	Data inventory/mapping	3.6	Obtaining consent	3.44
Maintain Art. 30 records	3.48	Maintain Art. 30 records	3.42	Conducting DPIAs	3.35
Conducting DPIAs	3.36	Data subject requests	3.37	Int'l data transfers	3.31
Operationalizing RTBF	3.34	Conducting DPIAs	3.33	Data subject requests	3.3
Data subject requests	3.34	Operationalizing RTBF	3.26	Operationalizing RTBF	3.21
Establish legit interest	3.14	Establish legit interest	3.18	Establish legit interest	3.08
Data portability	2.88	Data portability	2.92	Appoint DPO	2.85
Appoint DPO	2.87	Appoint DPO	2.9	Data portability	2.79

risk of not appointing a DPO, 31 percent of all respondents – and 35 percent of EU respondents – responded with "maintaining the status quo," suggesting they are already in compliance. The next most likely response is to increase privacy staff, which 23 percent overall plan to do, including 26 percent of those in the EU and 22 percent of U.S.-based respondents.

For all the other risks of non-compliance, the number one risk mitigation choice is clear: training, training and training. Respondents selected "investing in training" as the number one risk mitigation response for all but the DPO risk.

Among the GDPR-compliance responsibilities that carry the most risk for non-compliance, the second most likely risk mitigation choice is investing in technology. This conforms with the results from the 2017 IAPP-EY Privacy Governance Report, where privacy technology solutions leapt into the number two spot for GDPR preparation techniques, from eighth in 2016, now just behind training at number one.

For activities like conducting DPIAs or managing data subject requests, which may already be more familiar territory for privacy professionals (especially in the EU), after investing in training they plan to maintain the status quo and hope it meets the GDPR requirements.

People get ready, there's a train a-comin'

The GDPR was finalized approximately 18 months before it will come into force. While that seems like a long time, it has caused organizations to ramp up privacy budgets, add privacy staff, spend money on new technology, and – as mentioned above – increase privacy training across the board. Even with all that, a significant percentage of companies still believe they will not meet the deadline.

Americans love their lawyers

For the most part, whether headquartered in the U.S. or the EU respondents agreed on the appropriate risk mitigation response for the various GDPR non-compliance risks. If they tended to differ at all, it was in their likelihood to hire outside counsel, or to maintain the status quo. Privacy professionals in the U.S. were directionally more likely to engage outside counsel in several areas, including in preparing for breach notification, where 17 percent of U.S. respondents would rely on lawyers compared to only 9 percent in the EU. These margins held true across eight of the 11 risk areas. By contrast, EU respondents are more likely in each case to either invest in training or maintain the status quo, rather than hire outside counsel.

Outside legal counsel is most likely to be engaged when the risk involves interpreting the notoriously complex language of the GDPR. For instance, engaging outside counsel was the third most likely risk mitigation plan for international data transfer requirements, operationalizing the right to be forgotten, and establishing legitimate interest. Counsel is not likely to be engaged for typical in-house responsibilities like data inventory and mapping, maintaining records of processing, or conducting DPIAs.

Ranking of How Organizations Will Mitigate Risk

The biggest barrier to compliance by May 25, 2018, according to 32 percent of respondents, is the sheer complexity of the GDPR. This outcome was heavily influenced by respondents from the U.S., 38 percent of whom rank "complexity of law" as the top barrier to compliance, while EU respondents name "inadequate budget" as their top compliance hurdle with legal complexity a close second.

One in five respondents listed "too little time" as their stumbling block, and about the same number cited lack of qualified staff. Fewer than 10 percent overall say a shortage of technical tools is the "biggest" barrier to compliance.

While Americans may be struggling with the GDPR's complexity, they are nonetheless marching ahead toward compliance, estimating they are 49.27 percent of the way toward compliance, similar to the EU respondents at 47.31 percent and the overall response of 48.62 percent.

Respondents headquartered in the U.S. also project a higher likelihood than their EU counterparts of bringing their organizations into compliance with the GDPR by or before the May 25, 2018 deadline.

The effects of size and industry

When we explore the effects of company size and vertical market on how privacy professionals perceive risk, we find large unanimity. However, there are a couple of interesting notes.

Barriers To Compliance

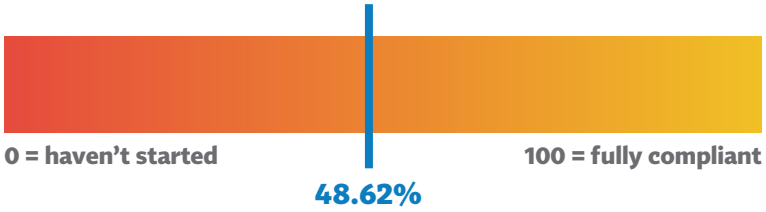
	Regulated (N=92)	Unregulated (N=290)
Complexity of Law	27%	33%
Inadequate budget	26%	21%
Too little time	19%	20%
Lack of qualified staff	20%	18%
Tech tools	9%	9%

continued on 9

Biggest Barriers to GDPR Compliance

Overall		U.S.		EU	
Complexity of law	32%	Complexity of law	38%	Inadequate budget	25%
Inadequate budget	22%	Lack of qualified staff	20%	Complexity of law	24%
Too little time	20%	Too little time	18%	Too little time	22%
Lack of qualified staff	19%	Inadequate budget	17%	Lack of qualified staff	18%
Shortage of tech tools	9%	Shortage of tech tools	7%	Shortage of tech tools	10%

How Far Toward GDPR Compliance



Expect To Be GDPR Compliant By...

	Overall	U.S.	EU
By end of 2017	7%	7%	7%
By end of March 2018	29%	**36%**	24%
By May 25, 2018	41%	**41%**	41%
After May 25, 2018	17%	9%	**24%**
Not sure	6%	7%	4%

Many organizations are making a big push in the last quarter of this year and the first quarter of 2018, with 36 percent of all respondents expecting to be GDPR-compliant by the end of March 2018, and another 41 percent saying they'll be ready by the May 25 deadline. This 77 percent total saying they'll be GDPR compliant by the deadline is one of few major deviations from the Privacy Governance Report. As the surveys were fielded six months apart, it is clear that some of the fear of GDPR has abated and now that privacy professionals have engaged with the compliance tasks they are finding them less intimidating.

Surprisingly, 84 percent of U.S. firms now say they'll hit the mark on May 25, 2018, while more than one in four EU organizations

continued from 8

For example, preparing for breach notification ranks as the highest non-compliance risk among both industries that are traditionally accustomed to privacy regulations – so-called "regulated" industries such as banking, finance, insurance, healthcare and pharmaceuticals – and those for whom the GDPR represents the first major privacy compliance lift (we call them "unregulated" industries such as software, business services, telecommunications and the like). However, unregulated industries rank international data transfers a close second non-compliance risk, whereas it is in sixth place for the regulated industries. Conversely, regulated industries are more concerned with data subject requests than those in the unregulated industries.

Unregulated industries are also directionally more likely to find complexity of the law a stumbling block to

Barriers To GDPR Compliance

# of Employees	Up to 999	1,000-24,999	25,000+
Complexity of Law	28%	29%	**40%**
Inadequate budget	23%	23%	17%
Too little time	18%	24%	14%
Lack of qualified staff	19%	16%	22%
Shortage of tech tools	12%	8%	7%

continued on 10

don't have confidence they'll be in full compliance. Apparently, lack of budget is a higher hurdle to overcome than a law's complexity alone.

Conclusion

For privacy professionals still feverishly ramping up for GDPR's launch next May, there may be comfort in knowing … you're not alone. Whether an organization is in the U.S. or the EU, the law applies to the large majority of organizations. Many find it complicated, and must prioritize which of its requirements they will tackle first. The consensus seems to be that privacy professionals – many of whom already wear the DPO hat—should be working on data inventory and mapping along with preparing for breach notification, working with marketing on customer consent issues, and installing or updating mechanisms for lawful international data transfers.

Because of the GDPR's scope and complexity, moreover, employees throughout the enterprise must adapt their practices to meet its requirements. This requires new data protection policies and practices, as well as training to create knowledge and awareness of those policies and practices. For some tasks, installing privacy technology will assist with compliance while in many other cases legal advice will be needed to inform program design.

Privacy professionals in the EU, accustomed to data protection practices under the Directive, may find their programs require less adaptation overall and are more comfortable with the status quo. And yet, nearly a quarter of European organizations say they will not be ready by the deadline. One wonders if they are less fearful of enforcement actions, or simply do not have the budget to reach the goal on time.

continued from 9

GDPR compliance, and somewhat less likely to blame an inadequate budget.

When we look at companies by size, moreover, we find risks are ranked in much the same order regardless of size, and mitigation strategies are similar across the board. The largest organizations (more than 25,000 employees) were highly likely – nearly 40 percent – to cite complexity of the law as the biggest barrier to GDPR compliance. Mid-sized organizations – between 1,000 and 25,000 employees – were more likely than the largest ones to cite a lack of time as an excuse for non-compliance, although they were just as likely as the largest organizations to expect to meet the May 25, 2018 deadline.

Expect To Be GDPR Compliant By...

# of Employees	Up to 999	1,000-24,999	25,000+
By end of 2017	**17%**	3%	1%
End of March 2018	30.5%	27%	32%
By May 25, 2018	30.5%	**45%**	**46%**
After May 25, 2018	19%	18%	14%
Not sure	3%	7%	7%