GDPR BENCHMARK REPORT

A VIEW FROM THE FINANCIAL MARKETS

According to new findings from a Cordium and AmberGate survey, more than half of investment firms are unlikely to be ready for the European Union's new General Data Protection Regulation (GDPR).

The survey conducted in April shows more than one-in-three respondents have not started their GDPR compliance projects. Nearly 22% of respondents are only one-third of the way through their program. Firms leaving their compliance responsibilities to the last minute may need to focus on key priorities of their program.

The findings are based on a survey of 279 responses conducted online and via a webinar between early and mid-April 2018. Asset managers make up 38% of responses, and hedge funds another 27%, while private equity funds composed nearly 15% of responses. A majority of respondents have operations in Europe (70%), closely followed by North America (40%) and Asia (10%). Not surprisingly, firms with reported operations in Europe are the most advanced with their GDPR compliance programs, with more than 18% saying they are either two-thirds or more complete, or finished.

FIGURE 1: Please select the option that most closely aligns with the type of firm you represent. (N=276)

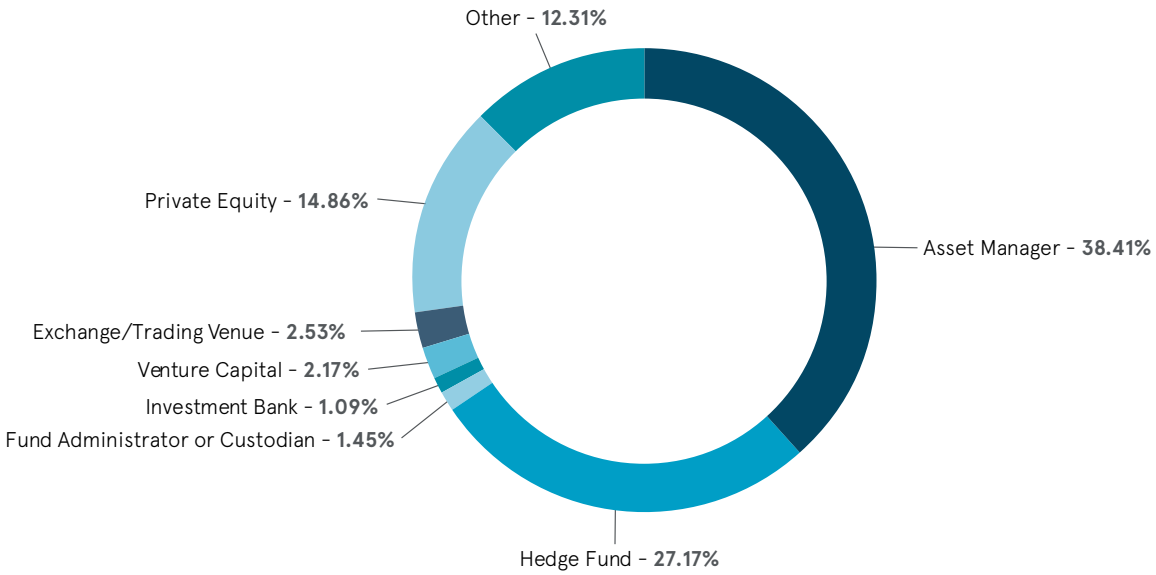
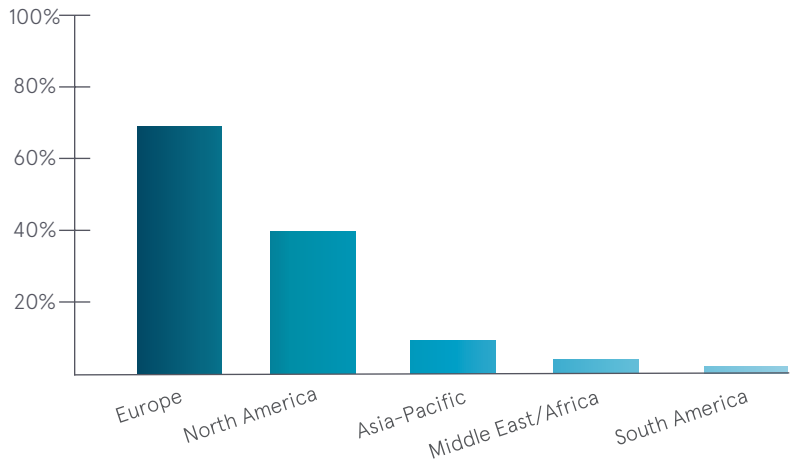


FIGURE 2: In which region(s) is your organization present? (N=263)



*Respondents were able to choose more than one category.

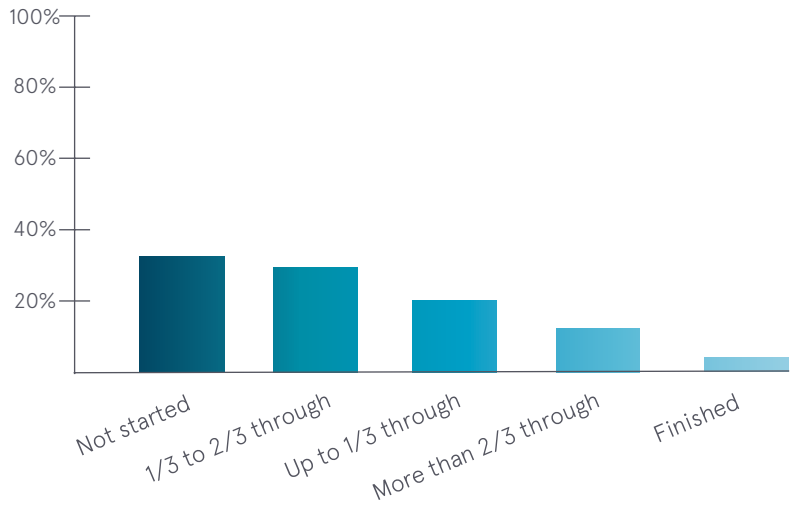
SIGNIFICANT NON-COMPLIANCE RISKS

All but the smallest and most simply structured of firms will struggle to complete their entire GDPR program within four weeks, without diverting significant resources and time to the project – there is simply too much to do across most organizations.

Firms that have not started their GDPR program – or who are only in the earliest stages – could be exposing themselves to significant compliance and reputational risk. If, after the May 25, 2018 deadline, such a firm is the victim of a breach, or experiences whistleblowing by a disgruntled employee, the regulatory penalties can be substantial – up to 20 million euros, or 4% of annual turnover, whichever is greater. The headlines that a non-compliance regulatory sanction will generate may also significantly challenge the firm's reputation and its relationship with its clients.

In addition, questions on a firm's GDPR compliance are becoming more common in due diligence questionnaires by investors and other stakeholders. Certain firms are more likely to be asked such questions given their activities.

FIGURE 3: How far through your GDPR compliance project are you? (N=229)



Nearly 30% say they are between one-third and two-thirds of the way through their program, while fewer than 14% of firms are more than two-thirds of the way through, in spite of the deadline being just one month away. Less than 2% of firms across all asset classes and geographies have finished.

Among asset managers, hedge funds, and private equity firms, the hedge funds came out as least prepared, with 46% not having started yet and nearly 24% just one-third of the way through. Almost 30% of asset managers have not yet begun, and just about 21% are one-third complete with their programs. Private equity firms are doing better – although 29% have not started and 23% are one-third of the way through, almost 23% are two-thirds or more complete. This compares positively against asset managers (14%) and hedge funds (8%) which are two-thirds or more complete.

Private equity firms may be further ahead in their GDPR preparations because of significant fundraising in the sector over the past 12 months. Today, more savvy investors are asking about GDPR and privacy preparedness, and so private equity firms may have been forced to act.

In addition, private equity firms are exposed to the risks and operations of their portfolio companies. Some of those companies may be greatly impacted by GDPR – for example, retail and technology organizations – and so private equity firms may be more aware of their compliance obligations as a result.

The remainder of responses composed of fund administrators/custodians, investment banks, corporate entities, exchange/trading venues, and others. Of all respondents, nearly 70% have operations in Europe. It's important to note, however, that GDPR has significant extraterritorial implications, because it applies to all organizations that offer goods or services or monitor the behavior of individuals within the EU - which is why firms with operations in Asia-Pacific, North America, and other regions also participated in the survey and attended the webinar.

PRESSURE FROM INVESTORS TO RISE

The survey found that, at the moment, the most pressure to comply with GDPR comes from firms' own internal governance functions – at nearly 45%. However, regulatory pressures are also strong, with 39% of respondents indicating that they are feeling the heat. Investors and customers are also proving to be an influential group, with more than 15% of respondents saying they are the source of the most pressure.

FIGURE 4: At present, which area generates the most pressure to comply with GDPR? (N=243)

This GDPR compliance pressure from investors and customers is likely to rise post-deadline – particularly as firms move into the fundraising part of their business cycle. No firm wants to have to tell an investor or customer that their GDPR compliance program has gaps, or that their overall approach to data security and privacy is not robust. Already, many firms are seeing queries come in from investors and customers about their relative state of GDPR readiness.

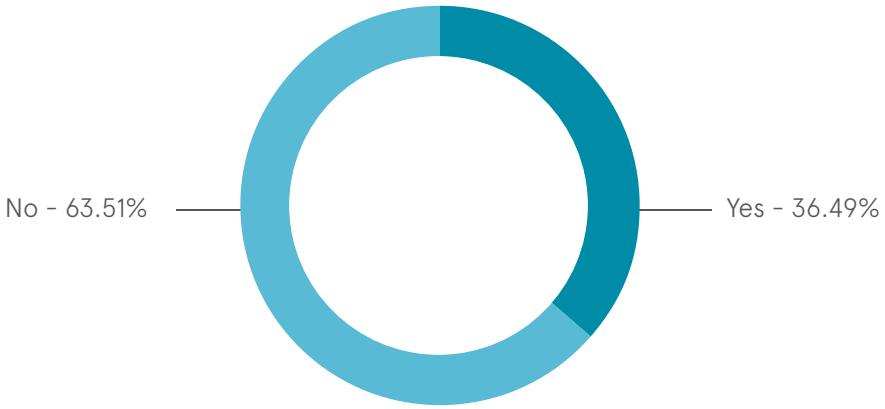
There will be pressure from regulators too – in its annual business plan for 2018/2019, the UK's Financial Conduct Authority has said it will review firms' use of data. In addition, the Information Commissioners' Office has been – and plans to continue – ramping up its enforcement staff.

RESPONDING TO A BREACH

Looking at specific issues, it's clear that most firms in this sector have a lot of catching up to do. The majority of firms – nearly 59% - are not ready to report a data breach within 72 hours. This is a hard and fast requirement when GDPR comes into force on 25 May; regulators have indicated that this is an enforcement focus. Firms can suffer catastrophic reputational damage if they fail to comply.

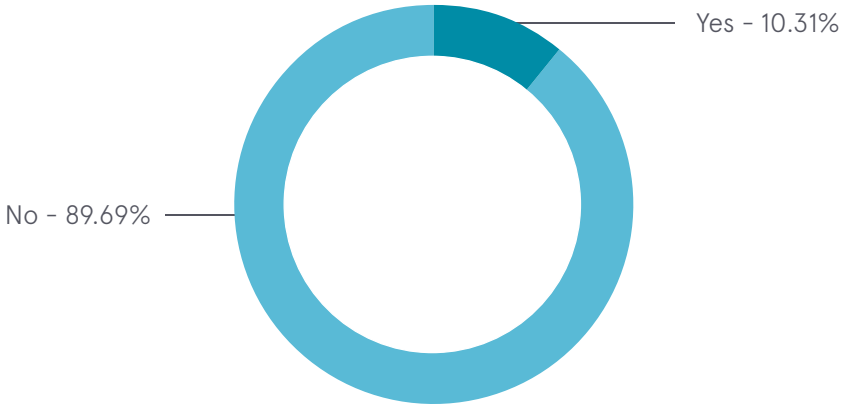
There are other areas where firms are lagging behind too. Just slightly more than 36% have practices and procedures in place to respond to an exercise of data subject rights, including erasure. Nearly 64% do not have these elements of their program in place. While most investment firms would probably not be subject to the kind of customer-based complaint that a request that a retail-oriented company might be, a possible source of risk is disgruntled employees or former employees. Human resources teams hold a wealth of personal data today. This can range from traditional information such as annual reviews, to more cutting-edge HR tools such as psychological evaluations – all of this is personal data.

FIGURE 5: Do you have practices and procedures in place to respond to exercise of data subject rights including erasure? (N=222)



The good news is that, for now, GDPR seems not to be having as much impact on business revenues or fundraising in the investment sector as it is in other types of industries. In the Cordium and AmberGate survey, just slightly more than 10% of respondents say GDPR compliance is causing delays in sales or revenue growth. In contrast, 65% of businesses in a broader survey by Cisco say they are experiencing sales delays due to privacy concerns. However, many Cordium clients have reported receiving explicit requests for information on GDPR compliance, as well as data privacy policies and procedures from potential and existing customers. Firms gearing up for fundraising should be ready to produce these materials on demand.

FIGURE 6: Is GDPR compliance causing delays in sales or revenue growth? (N=223)



ACHIEVING COMPLIANCE IN ONE MONTH

With just one month to go, where should a firm focus if it is facing the GDPR deadline with little of its compliance project completed? While firms should ideally be completely compliant by May 25, 2018, there are some specific items they should be certain are in place by the deadline. Firms must move quickly to ensure they achieve complete compliance as soon as possible.

Five top priorities for GDPR compliance one month out from the deadline should be:

1. **Governance**

Most firms will need to review their Privacy Governance Model in light of GDPR – for example, to evaluate whether or not a data protection officer needs to be appointed, to ensure that appropriate policies and procedures are in place, and that relevant training is carried out. Other roles and responsibilities will need to be added to the organization as a result of GDPR. The first thing regulators will want to see is the documentation around the firm's Privacy Governance Model.

2. **Data subject rights**

Much of this is new to the EU's data privacy regime, and so most firms are unlikely to have policies and procedures in place to meet these requirements. Organizations need to be able to identify all of the personal data they hold, and then to be able to access it, correct it, and apply restrictions to it. They also need to be able to provide data portability, and to erase the data as part of the "right to be forgotten."

3. **Contracts with vendors and customers**

All of the organization's contracts where personal data are processed should be reviewed, with particular care taken with contracts where personal data is being transferred outside the EEA. Firms should also understand how the vendors they work with, who handle their data, are complying with GDPR.

4. **Data retention**

Firms need to review the data they are storing. Under GDPR, there is increased focus on not only minimizing the personal data you collect, but how long you store it (the `retention period'). Some types of personal data may be best deleted completely rather than trying to establish a legal basis for retention - for example, notes on birthday, religious affiliation or children's names in a CRM system. Firms should purge all unnecessary personal data, as well as all data that is at the end of its retention period. Although many firms will have some form of data minimization program in place, most will need to make their policies and procedures much crisper in the wake of GDPR.

5. **Data breach reporting**

Just as all firms have a business continuity plan, they now need a Personal Data Breach Response Plan to meet the new requirement to notify regulators and individuals of certain breaches within 72 hours without undue delay. Firms should also consider a review of their insurance cover to see if it needs to be amended in light of the higher fines and penalties under GDPR.

At a minimum, firms who must comply with GDPR need to complete a gap analysis in these areas. They must develop a remediation plan, and begin to execute on it as quickly as possible. It is also essential that this progress be documented in full, to be ready to share with regulators and auditors.

Overall GDPR is much broader than just the five items above, and has specific nuances that some firms will need to be aware of and act on. So firms that are just at the beginning of their GDPR implementation project should ensure that any plan they put in place addresses how these other elements will be reviewed and ameliorated as well. Firms further along should, at this one-month mark, review what items are outstanding in their overall GDPR project and the adequacy of the plans to meet the deadline. In short, GDPR is a significant project that many firms have already left very late, potentially opening themselves to considerable compliance and reputational risk.

ABOUT CORDIUM

Cordium is a market-leading provider of governance, risk and compliance services to the asset management and securities industry. Cordium has offices in London, New York, Boston, San Francisco, Malta and Hong Kong. The firm employs more than 200 experienced professionals who support over 1,500 clients in the financial firms industry. For more information visit **www.cordium.com.**

ABOUT AMBERGATE

AmberGate is a specialist data protection compliance consultancy based in London, UK. They assist clients in their GDPR and broader data protection compliance needs, through use of proprietary tools and products. For more information, please visit **www.ambergate.io.**

RESOURCES

Cordium's GDPR Consulting Services for Investment Firms

GDPR: What you need to know (On-Demand Webinar)

Non-EU firms and GDPR: Time to face up to compliance

GDPR – Ready or not, here it comes...