Data Management Review

FROM A-TEAMGROUP

How to Tackle the Challenges of GDPR

An essential guide to understanding and implementing the requirements of General Data Protection Regulation (GDPR)

Commissioned by asg technologies™

Introduction

Financial institutions around the world are bracing themselves for the onset of the EU's General Data Protection Regulation (GDPR), which introduces eye-watering financial penalties for firms failing to meet stringent new rules on managing the personal data of EU residents. From May 2018, businesses will be required to provide evidence of consent for use of an individual's personal data and meet requests from individuals to delete and correct errors in the information. Businesses must also provide regulators with copies of the data on demand.

The financial services industry collects and manages large volumes of personal data. As such, GDPR will have a major impact on the way financial services firms manage client and prospect information. While the regulation applies directly to entities operating within the EU, GDPR's requirements extend to any business globally that is collecting personal data from EU residents.

In fact, GDPR applies to every entity that holds personal data derived from activities subject to EU regulation anywhere in the world. Its global scope means firms that control or process data relating to EU and non-EU citizens residing in the EU will be forced to deal with complex regulations governing personal data.

GDPR presents extensive challenges, requiring businesses to fully understand how their client data is being used, where it is stored and who has access to it. Penalties for non-compliance are severe: ranging up to €20million or 4% of worldwide turnover, whichever is greater, for affected parties. As a result, GDPR is getting high-level attention.

With less than a year before the regulation takes effect, every business is under pressure to get its data-privacy house in order. To assess industry readiness and attitudes towards compliance, the A-Team Group conducted a survey of data management and data privacy executives at a range of financial institutions operating in the UK, Europe and the US. Survey respondent firms ranged in size from Tier 1 universal banks to Tier 3 asset managers, and ranged in function from large sell-side institutions and global custodians to investment managers and credit card processors.

This paper examines the data management challenges posed by GDPR for financial institutions and how they are responding. It also explores compliance approaches of these institutions, explains the importance of governance to successful compliance, and offers guidance on implementing new technologies to ensure compliance.

Executive Summary

- Survey respondents agreed that **GDPR will have a significant impact on business, requiring a review of personal data, how it is handled and applications that use the data. New approaches to data management will also be required**.
- **Firms without a central data repository find identifying and sustaining personal data challenging**. The same applies to building workflows for GDPR compliance.
- **Respondents stressed the importance of a robust data governance programme** to deal with the complexity of GDPR, and the challenge of identifying, monitoring and accessing personal data from a broad range of systems and platforms.
- Two-thirds of respondents admit compliance with GDPR will require **many workarounds to meet the May 2018 deadline**.
- GDPR text is published in 24 official EU languages, meaning different jurisdictions may interpret it differently. This could cause **difficulties in understanding the requirements and identifying the data required** to formulate a compliant solution across different jurisdictions.
- Anecdotally, several respondents said they plan to leverage existing compliance efforts around Anti-Money Laundering (AML) and formalize the procedures to meet GDPR's specific requirements.
- Survey respondents cited issues with compliance with GDPR and Know Your Client (KYC), AML and other financial crime / surveillance measures.
- Firms are looking to **source in-house solutions for GDPR** as far as they can, but they acknowledge the need to **look outside for specific elements** of functionality.
- GDPR is seen as a **cross-functional effort** across lines of business (LOBs) and legal, compliance, IT and finance departments.
- **Data Protection Officer (DPO)** – There was a **mixed response to the prospect of putting in place a DPO**.
- The main benefits identified were **ensuring regulatory compliance and reducing liability, plus reducing reputational risk**.
- **Overall message**: Financial institutions will meet the deadline but with workarounds as they are grappling with cross-jurisdictional challenges, understanding the regulation and identifying the data required. **There is much work still to be done**, but respondents concluded that use of **central data repositories will ease the challenge** of identifying and sustaining personal data workflows as required for GDPR compliance.

Compliance Challenges for Financial Institutions

GDPR is an EU regulation that builds on its predecessor, the Data Protection Directive, by attempting to harmonize obligations for protecting data privacy across all 28 EU member states.

GDPR requires a much more rigorous approach to protecting data privacy than its predecessor. At its core, is the understanding that while data is an asset, its ownership remains with the EU citizen and not with the data controllers or processors. This is particularly prescient in financial services, where much of the data held and managed by financial institutions concerns clients and their holdings and activities. As a result, financial institutions will be obliged to protect the rights of citizens introduced or reinforced by GDPR.

But, with many other highly specific regulatory imperatives in finance services – European Market Infrastructure Regulation (EMIR), Markets in Financial Instruments Directive II (MiFID II) and Basel's Fundamental Review of the Trading Book (FRTB), among others – it isn't clear that financial institutions are placing as much emphasis on GDPR as perhaps they should. As one survey respondent put it: "For firms like Google, Facebook and others who deal with consumers, and have a large number of consumer records, this would be very high on their list. As far as banks go, not so much."

Most financial institutions surveyed were familiar with many of the provisions included in GDPR through their Data Protection Directive compliance activities. But GDPR adds new structures to the requirement, breaking down the landscape into legal process owners or controllers, data controllers, data subjects, and data processors.

GDPR's main articles describe interactions between these stakeholders, and this set of parameters represents a significant challenge for financial institutions in terms of understanding the scope and granularity of what's required. Specific challenges include understanding what personal data is held within the organization, what business processes affect regulated data, and how data is handled and transported.

GDPR enhances the rights of individuals especially around the right to be forgotten. It governs data portability, data profiling, and the use of personal data in automated decision making. It increases the obligations on data processors to implement and maintain both conditional and technical measures to protect personal data. And it introduces the concept of privacy by design, which requires each new service or business process that makes use of personal data to take protection of the data into consideration.

This new complexity will require robust data governance. Firms need to understand where personal data is held, and how it flows between applications and processes. For example, GDPR's notification provisions require data controllers to inform data subjects how their data is being processed in a fair and transparent manner, and give the individual the right to withdraw data if they wish. This translates into a broad accountability requirement for financial institutions to keep records of how they process personal data and how they protect it. Moreover, firms need to respond to regulators' enquiries within 72 hours.

Although as a regulation GDPR doesn't require transposition into individual member states' laws, it will allow member states a degree of tailoring, with around 50 GDPR provisions allowing for local clarification or exception. This means GDPR is essentially multi-jurisdictional, making compliance a complex challenge.

Further complexity is introduced by issues around overlap with other regulatory initiatives. In particular, firms' efforts around addressing financial crime –AML and KYC compliance – appear to bring them into conflict with some of GDPR's data privacy provisions. Moreover, different rules in different jurisdictions mean that a firm could be compliant in one jurisdiction yet not in another.

GDPR comes into effect on May 25, 2018. Financial institutions report they are still far from compliant but are focused on the penalties for non-compliance. GDPR makes provisions for financial penalties of up to 4% of group annual revenue/turnover, with €20 million minimum per breach.

A Regulatory Response

GDPR's extensive requirements point to a compliance technology solution that offers a number of features. For example, the solution must be agile enough to support rapid response to regulatory ad-hoc queries. This agility is challenging due to the complexity and physical distribution of the personal data held within any given financial institution.

Firms need to be sure they are using the right data. Financial institutions hold many repositories of data, often with conflicting elements. They generate huge quantities of derived data, making rapid identification of all instances of use of personal data difficult. Finally, due to the base complexity and multi-jurisdictional nature of GDPR, it is difficult to prioritise and coordinate data management activities to ensure compliance.

Until now, privacy solutions have revolved around two types of approaches; Privacy Program Management and Enterprise Privacy Management.

Privacy Program Management provides automated privacy impact assessments, frameworks for implementing a privacy program, website scanning tools, vendor risk management tools, and services for demonstrating privacy compliance. These are typically designed for use specifically by data privacy staff.

Enterprise Privacy Management solutions provide broader capability and use automation and artificial intelligence techniques to scan and map company data assets, then apply tools for monitoring, managing, controlling, and auditing data access and flows.

GDPR takes the requirement a step further, by adding the need for classification of the widest possible range of data assets and identifying all repositories and processes associated with those assets. Because of the need to respond rapidly to regulators' requests for information about the use of personal data, it's essential to tag data fields containing 'private' data and trace all connections to applications and processes that use them.

Privacy by Design

This transparent understanding of the data itself, the applications that use it, and the transfer of personal data between repositories and applications underpins the concept of 'privacy by design,' which is required to meet GDPR's data provisions. Monitoring changes to both the personal data itself and the data environment is key to providing ongoing intelligence that maintains this level of understanding. While privacy by design must be applied to new applications and processes, implementing privacy by design to existing systems can be a challenging retrofit.

Privacy by design, according to one survey respondent from a major credit card processor, entails "implementing proper controls at the beginning of a product's life or client relationship. Do we have standards for data capture, are we storing it correctly, are access rights, governance in place? It's all about making sure access is correct." His advice: "Don't try to boil ocean."

This executive recommends using an established template like the one offered by the Information Commissioner's Office (ICO), rather than building from scratch. "Our own template became too large, we covered too much in it," he said. "There's a real danger of scope creep. It's about identifying risks of that data to the organisation. It needs to be signed off by product owner and privacy office. But it's a living document; it needs to be measured all the way through."

This privacy by design approach points to the need for a strong and stable governance program.

One respondent says, "The concept of privacy by design, the need to secure design authority, and the requirements of GDPR for basic notification within 72 hours, these all increase the requirement around data governance. You need to understand where your data is, how it flows, and how to access it."

Plans for Compliance

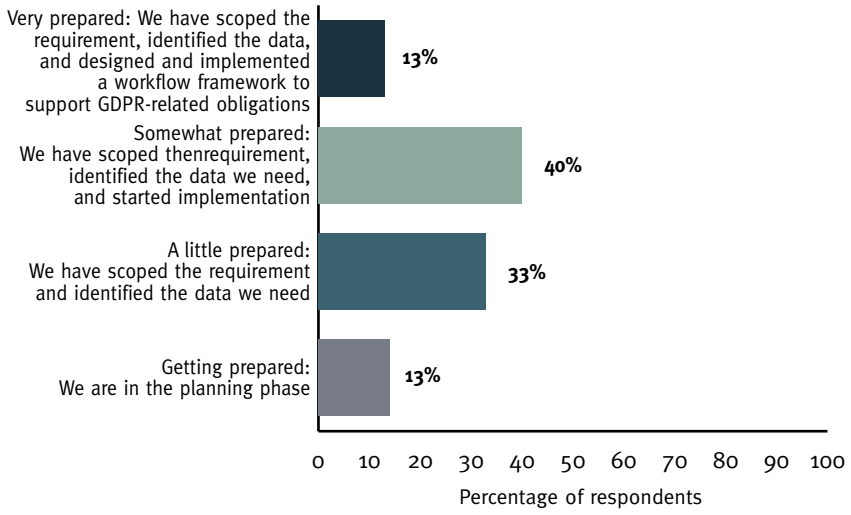
The A-Team Group survey asked participants about the key challenges of GDPR, their readiness and understanding of the requirements, and how they expected to achieve compliance. The survey also asked about governance, management buy-in, and how respondents intended to source data and technologies to meet the May 2018 deadline.

Understanding and Readiness

Respondents agreed that GDPR will have an impact on their activities, with 86% saying the impact would be significant as they work with many European residents. There was a more mixed response, however, about how informed firms felt about the regulation's specific requirements and their level of preparedness. Two-thirds of respondents said they were very well informed about the regulation's requirements, with the remainder saying they were somewhat informed, understanding the outline but less sure of the detail.

Under 15% said they were very well prepared to meet their obligations under GDPR. The bulk of respondents – 40% – claimed they were somewhat prepared, having scoped the requirement, identified the data they need and begun implementation. A third of respondents reported they had scoped their needs but had yet to start implementation work.

How far advanced is your organisation in its preparations to meet the data management requirements of GDPR?



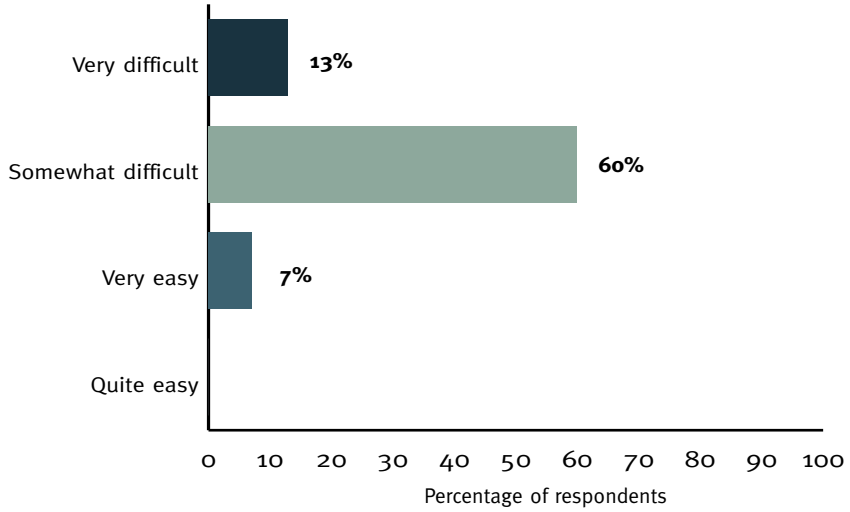
Some respondents expanded on how far along they were in the process of preparing for GDPR. One respondent from a major US bank said, "You need to set out your data needs. Who is controller / processor, what are the data elements, what is the purpose of the data, who are the recipients of the data, is it going overseas, is it being subprocessed? You need to answer all of this and demonstrate process when the regulator comes, usually after a breach. You need to show great process so that despite a data breach you can prevent a penalty. You need to demonstrate to the regulator what you're doing."

The main hurdle for this respondent was the regulation's complexity and the need to flag and categorize private data: "Thousands of applications, reports to regulators, lots of data sources, KYC. How do you approach knowing what you are doing with your data given this complexity? You don't want to boil the ocean but you need it to work. It needs something to look across all databases, but look at key processes and key systems for mapping, not just the data elements you store on your systems. You need to know what systems are using this data for and which other applications have access to it. It's not simple."

GDPR Data Challenges: Identification, Definition and Jurisdiction

Survey respondents acknowledged that their ability to identify and sustain private data will depend on existing infrastructure, particularly the presence of a central data repository. Firms without a central data repository said they were finding this aspect more challenging.

How difficult or easy will it be for your organisation to identify and sustain private data?



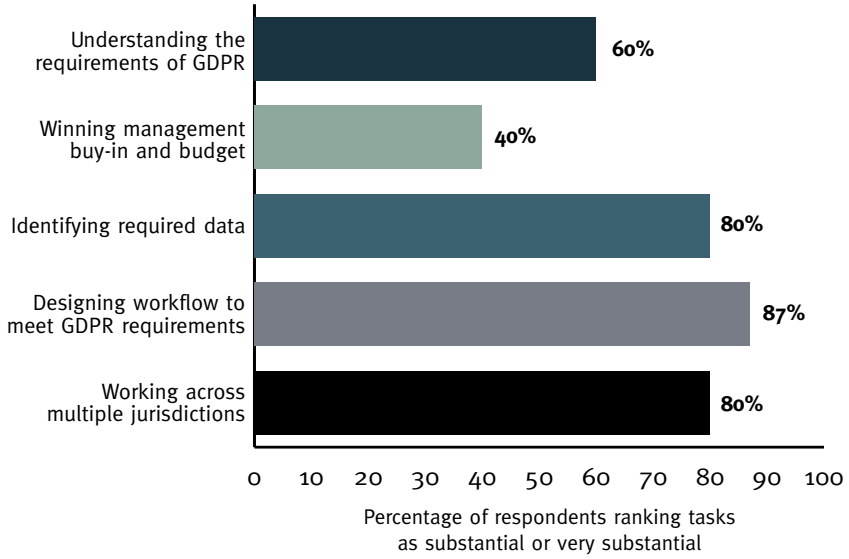
Towards two-thirds of survey respondents described the challenge of identifying required data as "somewhat difficult", with 13% citing the challenge as "very difficult." According to one respondent, a risk and compliance officer at a Tier 2 UK bank, identifying and sustaining personal data "will be very difficult because standards are high and the data is in a number of systems, and both of these things are key challenges of GDPR."

The head of data privacy at a major UK bank suggested that "although the requirements of GDPR are largely based on existing law, the requirement to demonstrate compliance makes GDPR a bit more of a challenge."

For another respondent, another risk and compliance officer at a Tier 2 US bank, "Identifying what is personal data goes back to what are the bounds of what you would say is personal and what isn't. I don't think there's an industry standard model that says which things are personal data. But there will be some discussion among the people who have to comply with this as to the bounds of what is personal and what isn't."

He continued: "If there were some kind of industry model that said this is what personal data looks like and most people agree with that, then it would be easy, but there's no such thing for banking. . . . If your email address is on 20 sites on the Internet, is it personal? It's a public piece of knowledge. There would be a lot of discussion on whether this is in or out. Obviously — name, address, social security number, phone number, passport number — those things are fairly easy and aren't even an issue. But there is a lot of peripheral stuff that people haven't really understood."

Rank these tasks in magnitude of workload



Just over half of respondents (53%) described the effort of designing workflow in accordance with GDPR provisions as "very substantial." One-third of respondents called it substantial. As one respondent, head of information security and data protection at a UK wealth manager, put it: "This will be somewhat difficult as we do not have a central data repository."

One of the major challenges of GDPR is that it crosses multiple jurisdictions, making it highly complex. This breadth of application makes the planning and implementation difficult across European financial institutions. Working across multiple jurisdictions was seen as a substantial challenge by 47% of respondents (with a further one-third assigning it a very substantial rating).

"Overlay GDPR's challenges with other jurisdictions and it becomes very complex," said a head of data privacy at a Tier 1 UK bank. "We need to give it structure that is meaningful when you are in front of regulators. That's the challenge."

Understanding GDPR's requirements and securing management buy-in were seen as less of an issue at this stage in proceedings, with just over one-quarter of respondents calling it a very substantial and one-third a substantial challenge.

Resistance from a Global Perspective

A further complexity lies in how non-EU firms should approach the regulation. European survey respondents with US parent companies, for example, said significant effort was needed to get management on board with GDPR compliance activities, as many felt the regulation applied only to EU firms.

One respondent says, "We get pushback from outside Europe; they don't want to be involved. But if they are marketing in the European Economic Area (EEA), then they are in scope. The initial assumption has been that they don't target the EEA. But [the bank] needs to clean up references to [product and service] availability in the EEA in order to circumvent the regulation. It's easier to look at data on a global scale than ringfence EEA data."

Others agreed that taking a global approach was preferable. "We do take a holistic approach and try to apply global standards where possible," said a respondent from a Tier 1 UK bank.

Seeking Further Clarification

There is uncertainty about the specifications. Survey respondents believe regulators will issue more guidance before the deadline. A full 80% of respondents said they expected further changes to the specification, in the form of additional "guidance and hopefully clarification," in the words of one respondent. Another added concern that "the ICO and working group are running late."

Some survey participants raised the issue of GDPR being driven by the information industry rather than financial services industry regulators. Said one representative of a Tier 1 UK bank, "GDPR is regulated by information regulators, and they have a different perspective. They are not used to the vast amounts of processing we deal with in financial services."

But there were workarounds here too. Added another, "Once you explain what you're doing, the need to comply with AML, etc., generally they get it. The difficulty is where they don't understand, and here we're using privacy by design tools to make sure we are doing this in a proportionate way."

Finally, one respondent suggested the Fifth AML Directive, for which no publication date has yet been set, "envisages big changes that could impact data protection."

Data Governance and Compliance

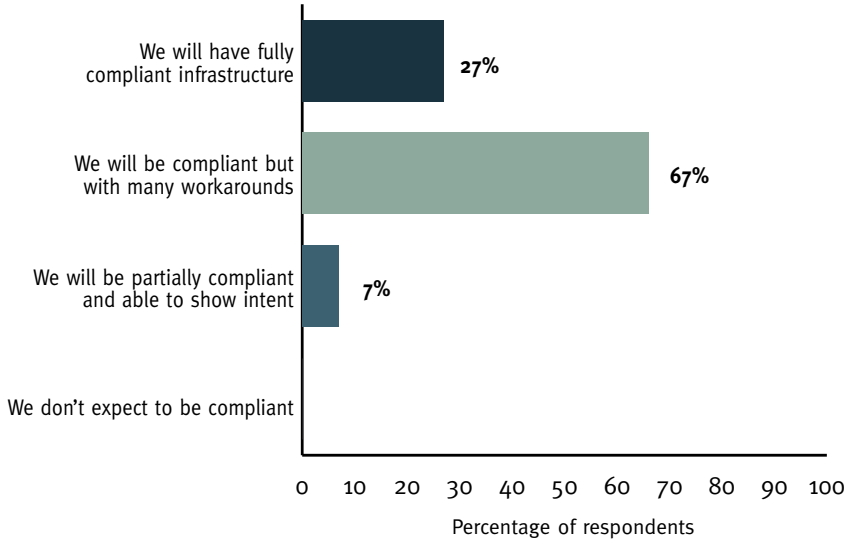
As described above, survey respondents stressed the importance of data governance in dealing with the complexity of GDPR. In particular, a robust governance program is seen as essential for meeting the challenge of identifying, monitoring, accessing and protecting personal data from a broad range of systems and platforms. As one respondent from a US Tier 2 bank put it, "The regulation doesn't list all the things that qualify as personal data. It talks about personal, professional and public. This could be fairly basic in terms of what we need to solve. But getting at all this data is a whole other story."

Despite the complexity of the challenge, almost all survey respondents said they expected to be compliant by the deadline of May 2018. The survey showed 27% expecting to achieve full compliance. Part of this certainty is down to the prospect of severe regulatory penalties for non-compliance – there is a sense that they have little choice. According to the Tier 2 UK bank risk and

compliance officer, “Firms can’t afford not to be fully compliant as there will be no leniency.”

While this certainty seems optimistic given the significant challenges firms are facing under a tight deadline, two-thirds of survey respondents admit that compliance by next May will require many workarounds, with the expectation that these workarounds ultimately will be replaced with a more comprehensive solution post-deadline. The single respondent not expecting to be compliant did expect to show intent, which was noted by others as important for avoiding regulatory penalties.

Do you expect to have infrastructure in place to achieve compliance with GDPR when it takes effect in May 2018?



Addressing GDPR Workflows

Respondents said creating workflows for GDPR compliance presented a major challenge, with 73% describing it as “somewhat difficult” or “very difficult.” Some firms were still finding it difficult to understand how to approach workflows, given the breadth of the regulation.

As one respondent described it, “The client can decide how we treat their data, so we need to slice up the cake and handle different slices as the client requires,” a process he described as somewhat difficult. The Tier 2 UK bank executive went further, “This is very difficult because the regulation is difficult to understand and because of the breadth of its application.”

Anecdotally, some respondents said they planned to leverage existing workflows from their AML activities. Said a compliance officer at a Tier 2 UK institution, “We are already doing this as we need to identify customers in line with AML… For GDPR, we just need to formalize our procedures.”

Finally, another respondent suggested technical deployment was the real issue, “Defining workflow would not be that difficult. Making it work on a technical level is a whole other story.”

Workflow Synergies and Conflicts

Survey respondents were keen to leverage synergies with other regulatory work where possible to progress their workflow efforts. But they were split, with 46% identifying some possibility of synergy (and one seeing significant synergies), but one-third suggesting only a few possibilities. Thirteen percent felt there was no possibility for synergies.

The optimists cited existing regulations like the Data Protection Directive, AML, and MiFID II. A respondent at a small UK asset management firm said, “There is a need to consider GDPR alongside MiFID II. MiFID II says what is needed in terms of data protection and GDPR says how to do it.” This respondent also cited connections with the Fourth AML Directive and the pending Fifth AML Directive.

Again, the multi-jurisdictional element of GDPR added complexity. While there is a single GDPR regulation, there are many iterations of it – at least one per EU country – inevitably raising the risk of conflict across versions.

To counter this, the head of data privacy at a UK bank suggested his UK teams could benefit from data privacy experience elsewhere. “Registration in the UK is easy; in Germany, Spain, France it’s an exhaustive process,” he said. “Data privacy teams in those countries probably have the best experience. We are trying to learn from them. They’ve had the data privacy officer role in Germany for some time; they’ve been far more rigorous.” Looking further afield, another respondent said there were synergies to be drawn from the US Bank Security Act, which had the highest relevant standards that applied globally.

Aside from the jurisdictional conflicts, survey respondents cited compliance issues with GDPR (and similar regulations in various jurisdictions) and KYC, AML and other financial crime / surveillance

measures. Lack of clarity from regulators meant that some were not sure which should take priority, leading to concerns about potential non-compliance for one or both.

The potential for conflict with financial crime activities in general posed challenges for respondents. “The conflicts between obligations to fight financial crime vs. data privacy are getting more difficult. This is not new. The barriers to sharing data are not just about data privacy, they also relate to bank secrecy, anti-money laundering, etc. But GDPR brings a sea change due to the 4% penalty. Before, maybe you’d take a risk; now, definitely not. It’s a game changer.”

This executive cited the Fourth AML Directive as an example. Coming into force in June 2017, the AML Directive was originally criticised for not referencing data privacy, and was subsequently modified to the point that it is now “littered with it,” according to this survey respondent.

At issue is that Article 45 of the AML Directive requires firms to put in place policies for data sharing given data privacy restrictions. In particular, it offers guidelines about what to do if the bank has a branch in a more restrictive jurisdiction and requires it to report where they are restricted from sharing by local data privacy laws.

The AML Directive’s requirement for firms to store records for five years conflicts with GDPR. Similarly, GDPR causes difficulty in data sharing with foreign regulators under the AML Directive’s newly extended reporting obligations. GDPR is complicating compliance with these and other AML provisions, says this survey participant. “Historically, we’ve relied on consent, public interest, etc.,” said this executive. “But it’s now more difficult to show legitimate interest, more difficult to obtain consent, and easier for individuals to withdraw consent. You need a clear understanding of what you are doing with the data and why. This is a major data management requirement. You need particular types of processes, and you need to know where the data is. There is no way to institute a legitimate process if you don’t know all this stuff.”

Key Functional Requirements for Compliance

Drilling down into the functionality required to comply with GDPR, responses varied across firms. Firms said they had deployed solutions to deal with certain aspects, among them: incident

analysis and reporting (73%); data lineage (64%); data retention / management (60%); data activity monitoring with blocking (53%); data masking, redaction or pseudonymization (53%); data discovery (50%); data classification (47%); and encryption (47%).

Some respondents believed themselves to be strong in particular areas: encryption (47%); data classification (40%), and data discovery (36%). Others said they were considering external solutions and support to help bolster their capabilities, with particular interest in data masking / redaction / pseudonymization (20%), data classification (13%) and data retention / management (13%).

Key aspects of the privacy challenge are new for many financial services institutions, according to the US bank respondent. “The masking and anonymizing of the data — before these regulations came along, banks were not prepared for this. For example, if they built a data warehouse to pull customer data together, they wouldn’t mask it. It would be your name, your social security number, whatever. It would just be based on the regular security. It would be another database that was secured in normal circumstances and they wouldn’t worry too much about it.”

The respondent continued: “But with all the new data privacy regulations, that information in the data warehouse, for example, it’s all masked and anonymized. They try not to actually store any privately identifiable information directly if they don’t have to. The way they’re storing things has changed and the way they’re securing it has changed in that they’ve actually taken the security down to the individual field levels rather than just putting a password on the database. Even if you got into some of these databases, you wouldn’t know who was in there.”

In terms of approaches on whether to anonymise or pseudonymize personal data, survey participants said they used both approaches. “Encryption, anonymization (which can’t be reverse-engineered), pseudonymization (tagging); that’s in descending scale in terms of privacy,” said one. “We are focusing on privacy by design, using techniques to make life easier, and you can use and share data more easily if you do this properly. For some functions we aggregate and anonymise pseudonymized data so it can’t be reverse-engineered.”

Technology Approaches

Just over half the survey respondents (53%) said their firms are looking to source in-house solutions for GDPR. These are likely to build on existing responses to the Data Protection Directive or will be implemented by smaller firms operating only in the EU and dealing with relatively low numbers of European residents. The remainder of respondents expected to implement a hybrid solution based on both in-house capabilities and vendor tools, as no single supplier was seen as able to meet all the regulation's requirements. Once again, the multi-jurisdictional nature of GDPR complicated the issue, with a solution for one jurisdiction not necessarily considered useful for compliance in another.

Among the respondents opting for a hybrid solution, a Tier 1 UK bank representative said, "We decided on a hybrid solution as we already have a lot of existing tools we can use. There are also data mapping tools from external vendors that we can use. If we identify any gaps, we will go to the market to look for tools to plug them."

Organization and Resource

Organizationally, GDPR was seen by most respondents as a cross-functional effort across lines of business (LOBs), and the legal, compliance, IT, and finance departments. Respondents said leadership roles tended to hail from compliance (90%), legal (30%), and IT (27%) departments. A small number of respondents said human resources were also included in their GDPR teams.

Some saw at least part of the GDPR requirement as the responsibility of the chief data officer. "Identifying the data – this is the remit of the CDO, who has a team of people who own things like reference data, what the terminology is, and what it means. Identifying what data we need is not that difficult, but seeing where it is, that's a different question."

Oversight seems to have been given to a data protection officer – or to the person within an organisation that has had that function added to his or her portfolio. Survey respondents gave a mixed response to the prospect of putting in place a DPO, with some planning to hire one (21%), some making the role part of someone's existing job (36%), others having no plan (30%), and others already having one in place (14%). In terms of overall GDPR resource and expertise, 47% said they had sufficient domain expertise and in-

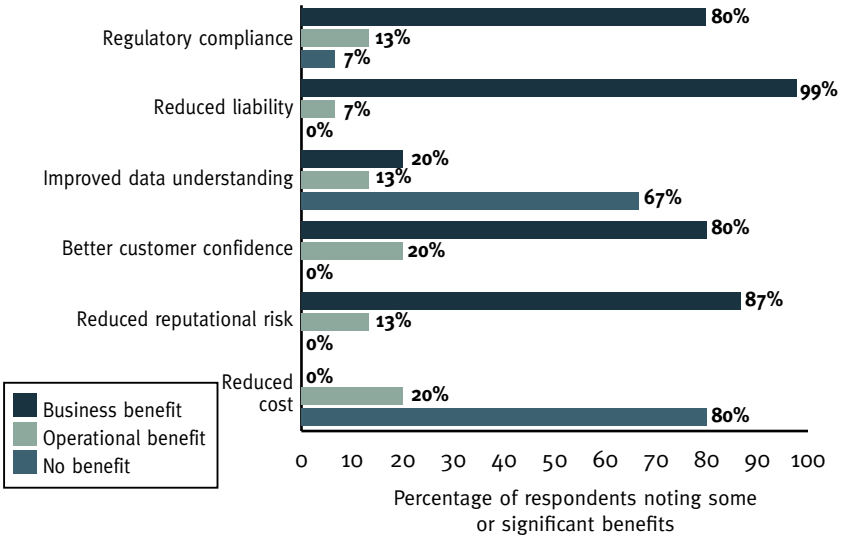
house resource to handle the regulation's requirements, with the remainder conceding that they needed to increase their resource in this area.

Recognizing the Benefits of GDPR Compliance

The main benefits that survey participants saw from their GDPR initiatives were ensuring regulatory compliance (two-thirds saw significant business benefit) and reducing liability (93%), as well as reducing reputational risk (87% saw either significant or some business benefit). Outside of the enforced nature of the regulation, the benefits were less obvious, with participants believing some benefit may come from better customer confidence (73% saw some benefit).

But most respondents saw no direct benefit of reduced costs or improved data understanding – attributing these to separate efforts – even though GDPR's stress on proper use and retention of data should result in greater understanding and optimization of data and data management resources.

What benefits does your organisation expect to gain from a successful implementation of GDPR and how significant will they be?



Robust Solution Required for Compliance

From the survey, the overall message seems to be that financial institutions will meet the deadline but with workarounds as they are grappling with the challenges of GDPR's multi-jurisdictional nature, understanding the regulation and identifying the data required. There is much work still to be done, but respondents concluded that use of existing – or deployment of new – central data repositories and other workflow tools will ease the challenge of identifying and sustaining personal data workflows as required for GDPR compliance.

While firms understand key GDPR concepts based on their experience with the Data Protection Directive and other regulations, they acknowledge that no single technology solution will fulfil all the regulation's many requirements. As a result, firms are building their own solutions, often using outside suppliers' functionality to fill gaps in their capabilities.

Finally, respondents suggested that governance would play a key role in a successful GDPR compliance programme. The complexity of the data requirement, the fast turnaround needed to comply with data notifications, and the multi-jurisdictional nature of the regulation all add to the challenge of identifying and accessing the right data at the right time in order to prove compliance.

To achieve this, data lineage and data governance tools that are robust, accurate and efficient are needed. The data lineage approach needs to be able to track data as it moves through multiple systems. It needs to be able to work with large data sets, with the capability to tag private data so that the firm is able to respond to queries about how that data is being used.

Finally, the approach needs to keep track of the evolving data environment, pointing to a requirement for a Big Data ecosystem that allows financial institutions to benefit from increased intelligence about the data they hold while minimizing risk of non-compliance.

By taking this approach to underpin a privacy by design framework, financial institutions can establish a robust GDPR compliance solution that minimises the risk of penalties while maximising the value of client data. Adopting a flexible framework also optimises the data management resource to deal with wider data issues going forward.

About ASG Technologies

ASG Technologies, the leading provider of information access, management and control for every enterprise, understands what it takes to enable digital business transformation. ASG Enterprise Data Intelligence is the only solution available to offer a zero-gap data lineage system at its core. This ensures that each data transfer is tracked and transformed with confidence. ASG unlocks the relationships between data items across the enterprise or individual lines of business. ASG Enterprise Data Intelligence builds a rounded understanding of data assets by adding business and technical analysis. With extensive data source coverage, data officers can trace the movement of data in data warehouses and big data environments on premise, in the cloud or distributed.

ASG Technologies' solutions empower businesses to enhance workforce productivity, gain an accurate and timely understanding of the information that underpins business decisions and address compliance needs with improved visibility of cross-platform data from legacy to leading edge environments. More than 70% of global Fortune 500 companies trust ASG Technologies to optimize their IT investments. ASG is a global provider of technology solutions with more than 1,000 people supporting more than 4,000 midmarket and enterprise customers around the world.

For more information, visit **www.asg.com**.

asg
technologies™

About A-Team Group

A-Team Group provides news and analysis, white papers, webinars, events and more through our two online communities:

- Data Management Review
  www.datamanagementreview.com
- Intelligent Trading Technology
  www.intelligenttradingtechnology.com

The A-Team Group also organise the RegTech Summit for Capital Markets 2017 taking place on October 5, 2017 in **London** and on November 16, 2017 in **New York**.

Sign up as a member free, download recent white papers, or look at our upcoming webinars and events and book your place today.

If you're a vendor and looking for high quality content – like this white paper – to help articulate your message, take a look at **www.a-teamgroup.com**.

Or get in touch: **020 8090 2055** / **theteam@a-teamgroup.com**.

Data Management Review

Intelligent Trading Technology

A-TEAMGROUP

To learn how ASG Technologies can delight your enterprise contact us at

Email: responses@asg.com

Website: www.asg.com/intelligence

asg technologies™