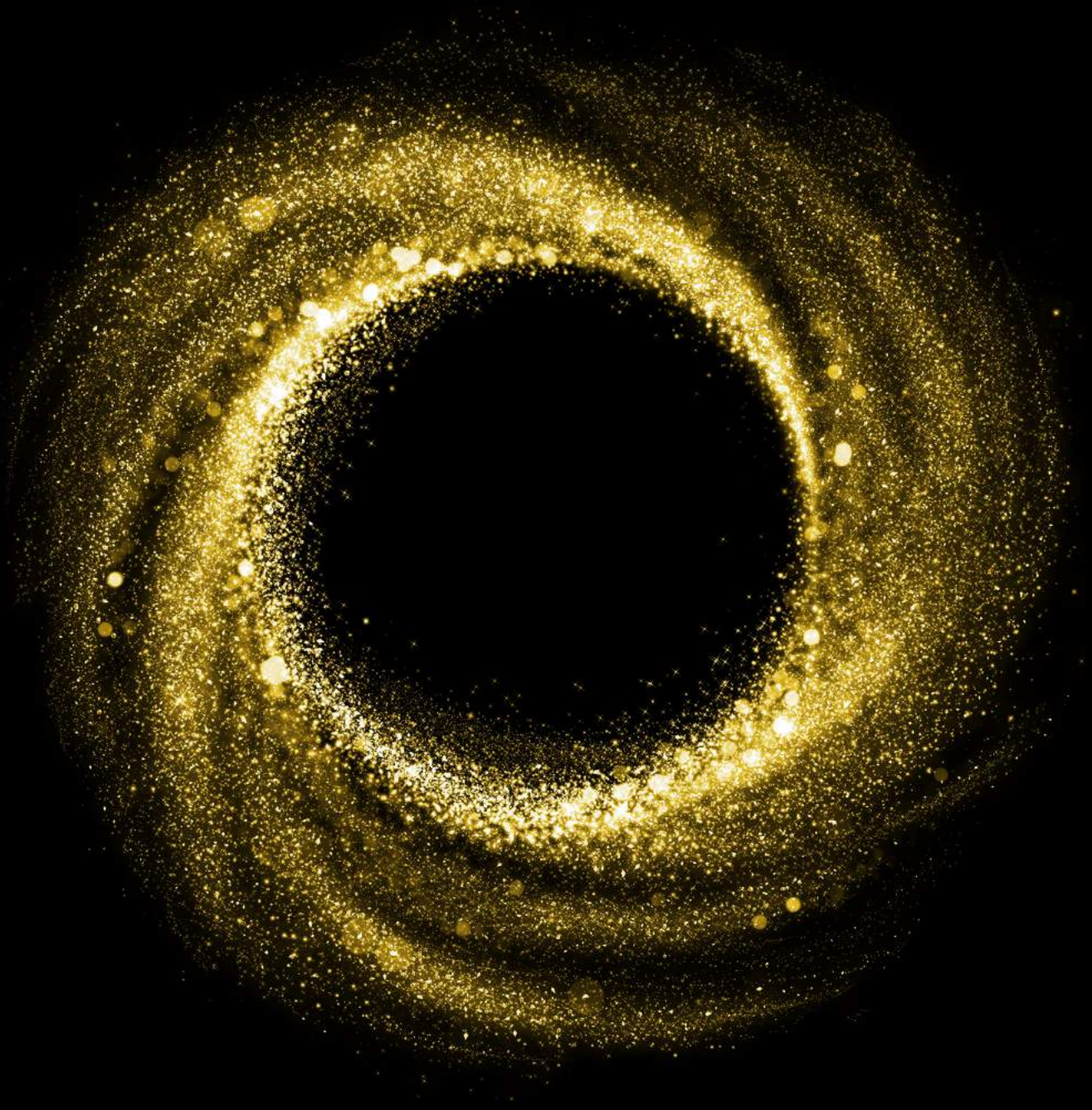
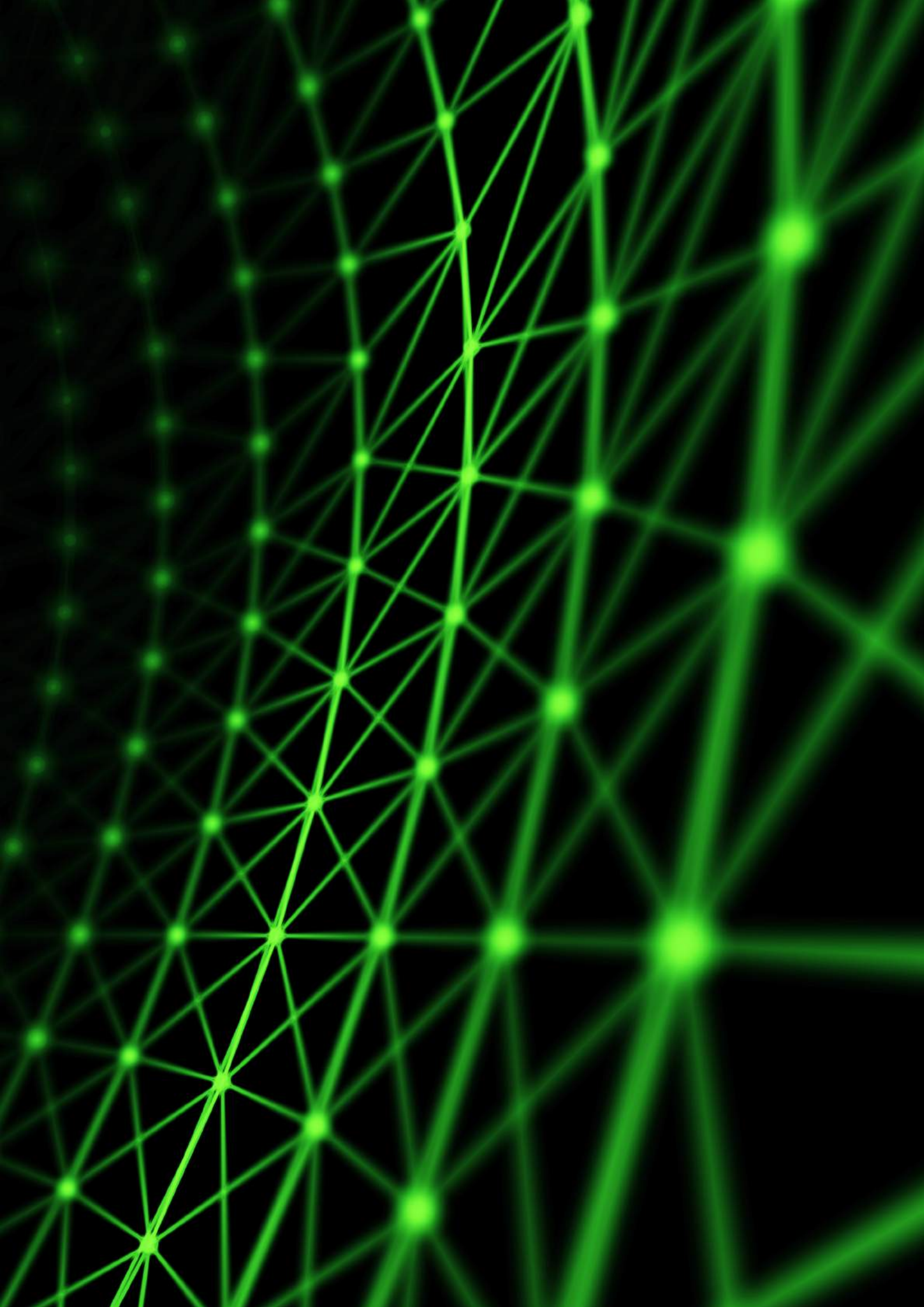
Deloitte.



After the dust settles

How Financial Services are taking a sustainable approach to GDPR compliance in a new era for privacy, one year on.

Contents



Our report finds that financial services companies have, in general, found it easier to comply with GDPR than companies in other sectors because of their long history of meeting strict privacy and data protection requirements set by financial regulators.

About this report

This report is based on interviews with data privacy specialists in Deloitte, financial services organisations, and the UK's Information Commissioner's Office. It also draws on Deloitte's November 2018 survey, A new era for privacy: GDPR six months on.

The 2018 survey elicited responses from 1,100 data protection specialists working in companies across all industry sectors in seven EU and four non-EU countries; this report uses only the responses from financial services companies in the seven EU countries – UK, Spain, Italy, Netherlands, France, Germany and Sweden.

Executive summary

The EU's General Data Protection Regulation (GDPR), which came into effect on the 25th of May 2018, regulates how organisations process the personal data of EU citizens. It improves the privacy rights of individuals and, among other things, requires organisations to report data breaches within three days. It can be difficult and costly to comply with. Penalties for non-compliance can be as high as €20m or 4% of annual global turnover, whichever is higher.

The regulation is supervised and enforced by the data protection authorities (DPAs) in each member state. The European Data Protection Board (EDPB), which is made up of representatives from each DPA and the European Data Protection Supervisor, ensures that GDPR is applied consistently throughout the EU.

Overview

This report looks at how GDPR has affected financial services companies and their personal customers in its first year of operation. It is a follow-up of Deloitte's November 2018 survey, A new era for privacy: GDPR six months on, which looked at the impact of GDPR on companies and their customers in all sectors of the economy.

This new report finds that, in general, financial services companies have more easily taken it in their stride than companies in other sectors. This is because they have a long history of complying with strict privacy and data protection rules set by financial regulators. Their strategic approach and detailed procedures are therefore likely to be more mature than those of firms in other sectors.

Compliance challenges

Despite generally being better prepared than firms in other sectors, financial firms have in many cases found GDPR compliance a challenge, because of its broad scope – affecting as it does so many departments, IT systems, and people – and the severe penalties for getting it wrong.

Particular areas of difficulty include managing data asset inventories, consolidating vast amounts of data into centralised pools, and complying with the way that GDPR has been interpreted in different ways by some EU member states.

Data breaches, regulatory enforcement and legal action

There have been no confirmed major data breaches by financial services firms since May 2018. However, there have been complaints to national data protection authorities about alleged breaches of GDPR by firms in various industries. Privacy International, the campaign group, has for example filed a number of complaints to the British, Irish, and French data regulators against several companies, including two credit rating agencies.

It is only a matter of time before financial services companies start to fall foul of the regulation and receive large fines. Class action lawsuits may also follow from groups of disgruntled customers.

Impact on business operations and commercial success

In some cases data protection measures have become so restrictive that they are impeding the operational effectiveness and revenue generating capabilities of businesses. Fortunately, this is less of a problem for financial institutions than for other types of businesses. However, there is a fear that it could stifle innovation in data processing by financial institutions, such as their use of artificial intelligence.

Consumer awareness

Financial services consumers are much more aware of their data rights now than they were under the previous EU rules. Many financial services companies have seen a slight increase in "data subject access requests" (DSARs) since GDPR came into effect. In answer to the 2018 survey question, "How has the volume of data requests changed since GDPR came into effect?," 65% of EU-based respondents said the volume of DSARs had increased. Similar numbers of respondents said that data portability, erasure, and marketing opt-out requests had also increased.

Technology-assisted GDPR compliance

Technology plays an important role in protecting data. When respondents were asked if they had invested in tools and technology to help them in eight areas of GDPR compliance, the responses showed relatively high levels of investment. They ranged from 68% who said they had invested in Data Protection Impact Assessments (DPIAs), to 79% who had invested in cookie compliance and 80% who had invested in unstructured data scanning. Even so, there is scope for much more investment in technology-based compliance tools. The Global CPO of a global bank stated that whilst a number of their GDPR processes are still manually operated, the intention is to fully automate them.

Executive management and board scrutiny

Executive management and supervisory boards in the financial sector tend to be better at monitoring their data protection policies and GDPR compliance procedures than their counterparts in other industries. This is because their organisations have evolved over decades to meet the strict requirements of a heavily regulated sector, where huge fines can be imposed on those that transgress.

The UK's Information Commissioner's Office does, however, have some concerns that executive management and boards in financial services companies may not fully understand their data protection compliance obligations and that their approach can be simplistic, with a focus on "tick-box" compliance with GDPR.

Recruiting specialist staff and training non-specialist staff

GDPR has created a huge demand for specialist staff, so much so that financial institutions have often struggled to meet their recruitment targets. This has been a particular challenge for the biggest companies which have had to appoint a data protection officer.

Non-data protection specialists dealing with personal data – such as customer relationship managers, marketing managers, sales managers and telesales operatives – have had to be trained in the basics of GDPR compliance and regularly reminded about the procedures and guidelines to follow. There is often a gap between what the data professionals understand about data protection and what customer-facing employees understand.

Has it all been worth it? And what's next?

Despite the high costs of complying with GDPR, the consensus is that a cost-benefit analysis would show the benefits to organisations are higher. When respondents were asked to rate the importance of eight drivers for GDPR compliance, they generally attached more importance to positive drivers, such as improving customer trust, increasing data processing efficiency, enabling an insight driven organisation, than to negative drivers such as the threat of regulatory fines. So it has been worth it for financial services companies, even before considering the benefits to customers.

As for the future, organisations should strive for a "data protection by design" approach, while recognising that there is no such thing as a perfect state of compliance. It is a constant process – the job is never finished.

1. Overview – the impact of GDPR on financial services firms and consumers

This report looks at how the General Data Protection Regulation (GDPR) has affected financial services companies and their personal customers since it came into effect on 25th May 2018. It is a follow-up to our November 2018 survey.

A new era for privacy: GDPR six months on, looked at the impact of GDPR on companies and their customers in all sectors of the economy, in seven EU and four non-EU countries. This second report draws on some of the findings from the 2018 survey – those relating to financial services – but it is based mainly on the views of Deloitte's data privacy specialists, as well as interviews with financial sector practitioners and the UK's data protection authority.

The financial services sector – a long tradition of compliance with data rules

Before we look at the quantitative results of the survey, what qualitative assessments can be made about the effect of GDPR on the financial sector compared with other industries? The consensus is that, in general, financial services companies have more easily taken it in their stride. This is because they have a long history of complying with strict privacy and data protection rules set by financial regulators. Their strategic approach and detailed procedures are therefore likely to be more mature than those of companies in other sectors.

Close monitoring by supervisors over the years has meant that banks, insurers, asset managers and other financial institutions are well attuned to the culture of data risk management and compliance with data protection regulations. Core structures have been in place for some time, so the effort needed to comply with GDPR has been modest and incremental rather than huge and sudden.

By contrast, non-financial services companies – those in retail, media or technology for example – are generally less mature in their approach to data privacy and protection. Some have almost had to start from scratch with their GDPR compliance programmes, as they did not have a privacy framework in place or a culture of privacy by design.

Survey responses

The answers to the **second question** in our 2018 survey support the opinion that the financial services sector has taken a more mature approach to complying with data protection rules than other sectors.

It asked respondents how much their organisation had invested in GDPR compliance. Looking at how financial services respondents in the EU replied, 51% said they had made some investment, ranging from *"significant"* to "*the bare minimum*," while 46% said they "*don't see compliance as a priority and have not invested to comply.*"

Respondents from all sectors replied entirely differently: 90% said they had made some investment, ranging from *"significant"* to "*the bare minimum,"* while only 8% said they *"don't see compliance as a priority and have not invested to comply."*

The explanation for this big difference is that financial services firms have for many years adhered to strict data protection regulations that have been set and enforced by their financial regulators. Compliance levels were already high for most of these firms; so high, in fact, that many did not have to make further investments to comply with GDPR.

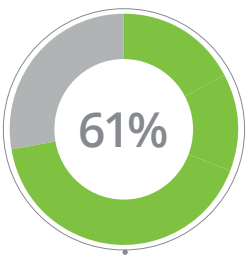
The **first question** in the survey asked people to rate the importance of eight drivers for their GDPR compliance activities. There were four possible answers: *"not a driver," "low importance," "medium importance"* and *"high importance."*

Respondents working for financial services firms in the seven EU countries gave *"Improving customer trust"* the highest score – 61% rated it of high importance. Next were *"Increasing efficiency in processing data"* (57%), *"Potential for reputational damage"* (56%) and *"Enabling an insight driven organisation"* (55%). *"Threat of regulatory fines"* received a high importance rating of 48%, placing it only seventh out of the eight drivers.

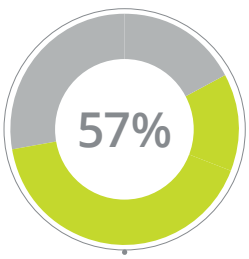
We can see, therefore, that respondents generally attach more importance to the positive drivers of GDPR compliance (improving customer trust, increasing data processing efficiency, providing insight) than to the negative drivers (worries about reputational damage and fines). This clearly shows that financial services professionals in general welcome the regulation more than they fear it.

When we look at the results from respondents in all sectors (financial services and all other sectors), there are similarities. *"Improving customer trust"* again scored the highest, with 56% rating it of high importance – but it was lower than the 61% given to that driver by the financial services respondents. Next were *"Potential for reputational damage"* (50%), *"Increasing efficiency in processing data"* (48%) and *"Threat of regulatory fines"* (47%).

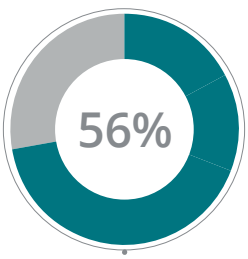
It is clear, therefore, that all-sector respondents attach slightly less importance to the positive drivers of compliance than financial-sector respondents. The reason for this could be that financial services firms have traditionally been more tightly regulated by their financial regulators and more closely complied with data protection laws, which over time has shown them that such a situation also comes with business benefits.



Improving customer trust



Increasing efficiency in processing data



Potential for reputational damage

Financial services sub-sectors

There are some differences in how various sub-sectors of the financial services industry have adjusted to GDPR requirements. Retail banks, for example, have adapted well, having traditionally invested heavily in compliance with previous data protection laws due to the nature of their business and the fact that they hold a vast amount of customer data. They are also used to being scrutinised by their regulators, much more so than companies in other industries.

Retail banks and insurance companies typically keep personal data for long periods in case it is needed in the future. GDPR stipulates that businesses must not keep personal data for longer than they need it, after which it should be erased or anonymised. So to comply with GDPR's principles of data minimisation, storage limitation and data retention, banks have had to change their mind-sets and review their customer records retention and disposal policies. As for retail customers' awareness of their rights under GDPR, most banks seem to be reporting a slight increase in data subject access requests (DSARs) since May 2018 but, in the UK at least, due to experience gained from the payment protection insurance (PPI) scandal, they have responded well.

Banks' capital markets businesses conduct relatively little business with consumers. They therefore hold low volumes of personal data and have not been heavily impacted by GDPR. They have found it easier to comply because the size of the task has not been so great.
However, there is also evidence of an overly relaxed approach to GDPR compliance by some US capital markets firms. US data protection standards have traditionally been lower than Western Europe's, especially Germany's. A cultural shift is needed if US firms are to match the standards of their European peers.

GDPR has not had as big an impact on the investment management sector as it has on the retail banking and insurance sectors because many investment management businesses operate mainly, or only, on a business-to-business (B2B) basis, rather than on a business-to-consumer (B2C) basis, and therefore do not hold as much personal data. However, the exception is the wealth management sub-sector of investment management, which deals with high-net worth individuals and where firms hold vast amounts of personal data, including special categories data.

Wealth management firms have made good progress in implementing processes for handling the expected increase in DSARs and have had few problems in dealing with them, as they are not a new concept. Nor have they had trouble complying with Article 6 of GDPR, which sets out the lawful bases for processing personal data. These bases, at least one of which must apply, include gaining the *"consent"* of the individual to process their data, a *"contract"* between the business and the individual and a *"legal obligation"* for the firm to process personal data to comply with the law (such as anti-money laundering rules).

A mature approach to managing compliance risk

Financial services have for a long time followed the tried-and-tested three lines of defence approach to compliance risk management: the first line being management control of frontline operations; the second being the risk management and compliance oversight functions; and the third being internal audit. The Data Protection Officer (DPO) in a bank or other financial institution sits clearly in the second line of defence. This mature approach to managing data risk is less common, or non-existent, in other industries.

The size of the fines levied in the recent past by financial regulators on firms that broke data protection regulations is another factor that has focused minds. It has ensured that GDPR has not been as big a shock to financial services executives as it has been to executives in other industries. When an insurance professional leaves a back-up disk in the back of taxi and the employer gets hit with a £1m fine, the likelihood of the same thing happening again in the future diminishes. Many lessons have already been learned about the importance of protecting data.

Noémie Papp, Head of Digital & Retail at the European Banking Federation (EBF) agrees.

"GDPR has been a key priority for banks. To comply with the May 2018 deadline they had to make adjustments to their technical tools and contracts and had to train their people. It's important for banks because trust is at the centre of the relationships they have with customers. Banks may not be trusted as much as they used to be because of the financial crisis, but in terms of data they are still really trusted. They are seen as gatekeepers for data. That is very important. Any data breaches would badly affect their reputation and client relationships."

Simon McDougall, Executive Director, Technology Policy and Innovation, at the UK's Information Commissioner's Office (ICO) says the regulation has had *"a huge impact"* on all financial firms handling personal data.

"However, in some ways the impact has been less dramatic in the financial sector than in other sectors because financial services firms were already highly regulated and used to dealing with big regulatory changes. For some organisations outside the financial sector, dealing with this kind of brand new regulation – which deeply affects how they do their business – was a new experience and therefore the shock was greater."

Banks that are primarily business or wholesale banks are still impacted by GDPR, as is pointed out by the data protection officer of the British subsidiary of one of Asia's biggest banks:

"We are a business-to-business bank and do not deal directly with personal customers. Nevertheless, we do have to take GDPR seriously because it requires us to protect not only employees' personal data, but business data that includes personal data."

"Where business data includes the names and phone numbers of business contacts, or email addresses that identify individuals, it is considered personal data under GDPR. There is no avoiding that. As a business bank we will not be under close scrutiny by the regulator, but we must still pay attention to the data we hold."

Kirsten Mycroft, Global Chief Privacy Officer of BNY Mellon, the global investments company, says that the priority now for many banks, 12 months on from GDPR implementation, is to ensure sustainable compliance.

"Banks have taken GDPR seriously and implemented meaningful changes to their controls and processes. Now the focus needs to be on ensuring that these changes are properly embedded into 'business-as-usual', that there is accountability and an effective operating model across the first and second lines of defence. That is really crucial. It's all very well to publish new policies and procedures, but unless they are properly embedded and sit within an accountability framework and an effective operating model, they may die a slow death."

A specific goal for global banks, says Ms Mycroft, is to consider all the similar regulations springing up around the world. *"Wherever feasible, we need to globalise and automate our data protection compliance efforts to accommodate the uplift in privacy regulations in areas like the US, Brazil, India and Asia-Pacific,"* she says.

"GDPR has been a leader in terms of a comprehensive data privacy and protection regime. Now it is driving other countries to consider what changes they want to make to their own privacy frameworks. Brazil's new law is similar to GDPR. India's proposed new law is also similar to GDPR."

"In the US, the California Consumer Privacy Act [which takes effect on 1 January 2020] has similarities, but it is not exactly the same as GDPR. If a bank is compliant with GDPR, it does not mean it will automatically be compliant with the CCPA. Other US states are also looking to introduce new privacy laws. The ongoing challenge for global organisations like BNY Mellon is to keep under review what their global baseline is for privacy and how to scale up and automate where necessary."

2. Compliance challenges

Despite generally being better prepared than firms in other sectors, financial firms have in many cases found GDPR compliance a challenge, because of its broad scope – affecting as it does so many departments, IT systems, and people – and the severe penalties for getting it wrong. So where are they tending to do well? What are they tending to do less well, and where do they come across difficulties - what can they do to improve?

Challenges well met

What they have done well, and have done so for years before GDPR came into force, is instilling a culture of compliance. Financial services firms are used to operating within a broad compliance risk management framework, into which privacy and data protection have slotted. That is not to say it has been easy. It has still been a challenge to get it right in many cases because of the complexity of their systems covering multiple countries and the volume of data passing through those systems in multiple countries. No matter how good your compliance framework is, there is a lot of data to manage and that is not a simple task.

GDPR requires companies to be more proactive in demonstrating compliance, as opposed to reactively answering questions from the regulator, and this is something that financial firms do well compared with firms in less regulated or unregulated sectors.

Data collection and analysis requires new and effective ways of using technology, much of it innovative. It requires automation; it may use artificial intelligence (AI) to analyse the data; and it requires data sharing on a wide scale. All of these uses of technology must comply with GDPR, which is something that financial firms are largely able to manage (see chapter 8 for more detail).

They are doing well on demonstrating accountability of board directors and executive managers (see chapter 5). They are doing well on staff training and awareness (see chapter 7). Financial services are used to the constant introduction of new regulations and all the training that goes with it.

Communicating privacy information to customers is a key requirement of GDPR. Organisations must be forthcoming with customers about the information they collect and hold on them, tell them why they hold it, and what they do with it. Financial firms have had to do this for years, and so have had little difficulty with the new rules. In the months, weeks and even days leading up to GDPR, a flurry of data privacy notices from non-financial services clogged up customers' email in-boxes. These firms had not properly prepared for GDPR, or had even been breaking the previous data protection rules; by contrast, very few, if any, such notices were sent out by financial services firms at the last minute because they had been meeting this requirement for years.

Under GDPR, businesses can only process personal data under certain conditions to ensure the processing is lawful. These include, for example, obtaining *"consent"* from the individual concerned, complying with a legal obligation, if there is a *"contractual obligation"* between the business and the individual, or if the company has a *"legitimate interest"* in processing the data. For Invesco, the global investment management firm, meeting these obligations typically did not involve getting in touch with its customers to obtain consent.

"In addition to complying with our legal or contractual obligations, we primarily relied on legitimate interests to process our clients' personal data, particularly in a business-to-business context, but, in some cases, we also utilised consent where it was the most appropriate legal basis for the processing," says **Martin Collins**, Invesco's Chief Privacy Officer.

Simon McDougall, Executive Director, Technology Policy and Innovation, at the Information Commissioner's Office in the UK, says financial organisations focused strongly in the build up to GDPR on people and processes.

"They were keen to make sure they could demonstrate accountability and that they had the right policies and procedures in place, for things such as privacy impact assessments, data protection impact assessments, and managing subject access requests."

Kirsten Mycroft, Global Chief Privacy Officer at BNY Mellon, believes banks in general have coped well with GDPR.

"Banks have taken it seriously," she says. *"We have had a lot of industry discussions about it and been thoughtful about the meaningful changes we needed to make."*

"At the heart of all of this is the individual. GDPR compliance strategies need to be client centric and employee centric to guard against 'tick-box compliance'. The other thing banks have generally done well is make sure they have executive sponsorship. Data privacy and protection should be a board level agenda item."

A problem for Royal Bank of Scotland (RBS) was the sheer size of its retail customer database and its legacy systems, but it was a problem it was able to overcome.

"Any organisation with a retail element to it has a lot of data, and we have huge volumes of customer records," says **Suzanne Rodway**, the bank's Head of Legal Operations and Data Protection Officer. *"Many data protection requirements existed under the old Data Protection Directive, but GDPR required a lot of enhancements which had a big impact on the larger, older banks. Challenger banks with only five years of data and tens of thousands of customers had a relatively easy task compared with us, with our 100-plus years of history, legacy IT and 18 million customers."*

Under the old rules, organisations had 40 days to deal with a data subject access request (DSAR) from someone exercising their right to find out how their personal data was being used and stored. GDPR cut that to 30 days.

"Our sector gets more subject access requests than any other, especially when you factor in those from claims management companies working on PPI [Payment Protection Insurance] claims. So losing 10 days off the cycle has been hugely impactful."

"Then we had to consider all the new rights that were granted under GDPR that didn't exist under the previous Directive like data portability and objections to processing. We needed to up-skill our frontline staff on how to handle all the requests, complaints and questions that we knew would come in. They cannot be dealt with in isolation. There are lots of moving parts. You need to know how privacy regulations interact with other regulations, and how not to upset Regulator A by doing something that is insisted upon by Regulator B."

Challenges harder to meet

There have been some pressure points for financial services firms. It has been far from easy. What many have found hard to get a grip on is managing their data asset inventories. The UK's Information Commissioner's Office spells out these rules in its *"12 steps"* to GDPR compliance: organisations should document the personal data they hold, where it came from, and who they share it with. An information audit may be necessary to ensure that data inventories are accurate and up to date.

Knowing where all this data resides is a huge task for firms, especially for large organisations that have grown through acquisition and have complicated and creaking legacy systems. Consolidating vasts amounts of data into a centralised pool would make inventory management easier, but such a task is itself a challenge.

In the **fifth question** of our 2018 survey, respondents were asked "How confident are you in your overall ability to proactively demonstrate compliance with GDPR requirements in the long term?"

Among the respondents working for financial services firms in the seven EU countries covered in the survey, 62% in total said they were confident, somewhat confident or very confident (6%, 19% and 37% respectively). By contrast, 91% of all-sector respondents said they were confident (respectively 38%, 32%, 21% for the three levels of confidence).

Why should companies in the financial sector be less confident than companies in other sectors, especially when in general they have had many more years experience complying with data protection laws and more in-house data privacy and protection staff? The most likely answer is that the former have a more realistic understanding of the difficulties of compliance than the latter, based on years of experience and first-hand knowledge of data breaches and the resulting penalties.

Perhaps the biggest compliance problem has been the way that GDPR has been applied in a non-harmonised way, says **Noémie Papp**, Head of Digital & Retail at the European Banking Federation (EBF).

"Fragmented regulation is a challenge," she says. "GDPR should be the same throughout the EU. But we still observe that different data protection authorities have their own views and have in certain cases implemented it differently."

GDPR allows some discretion as to how select provisions apply. For example, Data Protection Impact Assessments (DPIAs) must be carried out by organisations that are processing personal data that could be seen as a high risk for individuals, but what constitutes high risk will differ from country to country. The same can be said for notifying the supervisory authority of a data breach – organisations must report certain types of personal data breaches to the relevant supervisory authority within 72 hours of becoming aware of the breach, but the rules vary slightly from country to country.

"Every national data protection authority draws up its own list of the types of processing that need an impact assessment," says Hélène Benoist, Policy Adviser, Data Protection & AI, at the EBF. "This means that something that may require an assessment in one country may not in another. Processing could be classified differently across different member states."

Though it has dealt well with the compliance challenge, RBS has found it more difficult in some areas than others. Deleting data from many different, legacy databases is one example.

"There is a huge focus by the Financial Conduct Authority and the Prudential Regulation Authority on the security and stability of banks' IT systems, and changing one part of a system to meet data deletion requests could destabilise other parts," says **Suzanne Rodway**, RBS's DPO.

"Deleting large amounts of data is not as simple as it sounds. Banks that have been around for a long time are the product of many mergers and can have complicated IT infrastructures that they are trying to simplify. They are finding that data deletion is a detailed piece of work that takes time to complete whilst maintaining stability."

Relationships with data protection authorities

Many financial firms want to engage more with their national data protection authority (DPA). Others are reluctant to do so. Close interaction with the DPA should be beneficial because of the guidance they can provide.

DPAs tend to be smaller than financial regulators and are therefore not geared up or sufficiently staffed to offer guidance on as wide a scale. The increase in data breach incidents and complaints since May 2018 has further tested their resources. However, most have set up special interest groups or working groups to assist with the concerns of certain sectors, and it may be easier for firms to engage with their DPA collectively as opposed to a one-on-one basis.

"It is clear that dialogue between banks and data protection authorities is important," says the EBF's **Noémie Papp**.

"Banks are regularly in touch with them at national level. It is, however, important to keep in mind that since the implementation of the GDPR and even before, because data protection is a horizontal and cross-sector issue, some data protection authorities might find it difficult to deal with the increasing number of queries coming from consumers, SMEs, industry etc. Their resources remain limited and they have certainly been overwhelmed with requests for advice or information."

The UK's ICO has received many requests from small and medium-sized financial firms for advice on interpreting and complying with the regulation, mainly via its call centres.

"Larger financial institutions have large, well-resourced teams and they are able to deal with 99% of their challenges internally, which is as it should be," says the ICO's **Simon McDougall**.

"When larger firms do come to us, it's usually because they have something interesting to say on innovation which they want to discuss with us. We are building a regulatory sandbox for organisations, of all sizes and from all sectors, to test innovative products and services that will involve processing information about people and which will benefit them, their customers and society. It is, to some extent, based on the FCA's sandbox. It has just opened to applications. We will select approximately 10 applicants in late spring and go live in early summer."

"The relationship a financial institution has with the data protection authorities depends on what sort of institution it is. A retail bank that receives a lot of complaints from consumers will be on the regulator's radar, but wholesale banks with few retail clients and/or few complaints will largely be out of sight," says the data protection officer of a global bank.

"A bank with its main establishment in one European country, from where it does most of its business and makes most of its decisions, would have a much closer relationship with that country's data protection authority, which would be its lead supervisor, than we would. We don't have a lead supervisor because we have operations all over Europe, not in one central place."

Suzanne Rodway, RBS's Head of Legal Operations and DPO, says the bank used to have a close relationship with the Information Commissioner's Office, but *"the ICO doesn't have the bandwidth anymore" because of its increased workload due to GDPR.*

"I used to have routine catch-up meetings with ICO staff twice a year, and ad hoc meetings," she says.

"As GDPR came on the horizon they lost the ability to do that – because they had so much to do. We now deal with them through trade bodies like UK Finance and AFME [Association of Financial Markets in Europe]."

3. Data breaches, regulatory enforcement and legal action

To date, as far as we know, there have been no confirmed major data breaches by financial services firms since the 25th May 2018. However, there have been complaints to national data protection authorities about alleged breaches of GDPR by firms in various industries. Privacy International, the campaign group, in November 2018 filed a number of complaints to the British, Irish, and French data regulators against several companies, including two credit rating agencies.

It is surely only a matter of time before major GDPR breaches in the financial sector are confirmed, in which case large fines are likely to follow. The question is, how close to the maximum penalty – €20m or 4% of global annual turnover, whichever is higher – will those fines be? It would be surprising if any data protection authority pushed for the 4% turnover level for large financial institutions, considering the size of their turnovers, but we can expect the fines to be much higher than in the past.

The UK's Information Commissioner's Office previously had fining powers, but they were small. Some EU data regulators previously had no powers to fine. Now they have been given teeth, they can be expected to use them.

Although national financial regulators and data protection authorities (DPAs) will liaise closely on the imposition of fines, they do have separate powers. So it is possible that the local DPA could levy a 4% of global turnover fine on a firm, and the local financial regulator another fine of similar magnitude – a *"double whammy"*. Post-Brexit, a transgressor could face a *"triple whammy"* if the breach affected UK and EU citizens: a fine from an EU DPA, one from the UK's FCA, and one from the UK's Information Commissioner's Office under the Data Protection Act 2018 which implements GDPR in that country. It must be stated though that such scenarios are unlikely, with national regulators and authorities co-ordinating their responses to reduce the risk of extreme outcomes.

The biggest fines are more likely to be imposed on social media and advertising technology companies. EU and national authorities have already fined social media giants for breaking previous data protection laws, as well as for breaking existing anti-trust laws. Future similar data protection transgressions will result in much bigger fines.

Banks, insurers, and investment managers on the other hand are much more compliant. Although they hold a great deal of customer data, they do not use it as extensively, or for the same reasons, as social media companies, so the risk of non-compliance and large fines is lower.

The risk of a breach and a large fine is a genuine risk for retail financial institutions, believes RBS's **Suzanne Rodway**.

"My approach is, in relation to compliance, do I have a defendable position? I may not be able to guarantee I have got everything 100% right, but if I have tried hard to comply I have a position that is defendable. The ICO will punish those who don't care or are not trying, but not those who are trying to get it right and have just missed something."

Class action law suits

In addition to regulatory enforcement and fines, companies also risk class action law suits from consumers demanding significant compensation in the event of major breaches. These can be difficult to defend. Several such class actions have already started against major European companies, though they are not in the financial sector. It will only be a matter of time before cases start to be brought against financial firms, but the higher standards in the financial sector is keeping the safe for the time being.

It will be instructive to see where such actions lead, how they progress through the courts, how much of a battle there will be, and where the courts settle on the impact of the breaches on individuals.

The key question a court will ask a company is, did it do enough to protect its customers' data? The court may accept that there is no such thing as perfect security, but it will want to know if a company's data protection policies and processes were adequate to prevent most breaches and how well it responded after a breach to minimise the negative impact on individuals. If it finds the company lacking, the penalties are likely to be high. Compensation for each individual may be small, but added up across thousands, or hundreds of thousands, of plaintiffs the total would be far higher.

The class actions currently being brought may take another 12-18 months to complete, and when they do they will set precedents for the level of liability companies are expected to shoulder.

In the UK, the Payment Protection Insurance (PPI) scandal showed how easily lenders could infringe consumer rights, and then get punished for doing so to the tune of £33bn and still counting. The PPI claims process comes to an end in August 2019, so the claims management companies who handled most of them will be looking for other complaints to latch on to. While PPI claims were handled individually, if data breaches become a profitable new source of income for claims management companies they may well decide to pursue some of them as class actions. They have years of experience gathering evidence against banks and the ability to drive large volumes of claims. Perhaps, though, they may be inhibited by the fact that it will be harder to attach a monetary value to a person's data loss, whereas with PPI there was a monthly premium to start from.

In addition to class actions from consumers, there is also the risk of legal action from individual corporate customers. If a direct marketing company, for example, loses personal data provided to it by the client, it could allege breach of contract.

Suzanne Rodway, RBS's Data Protection Officer, says she is waiting to see how class actions develop, because no-one knows at the moment.

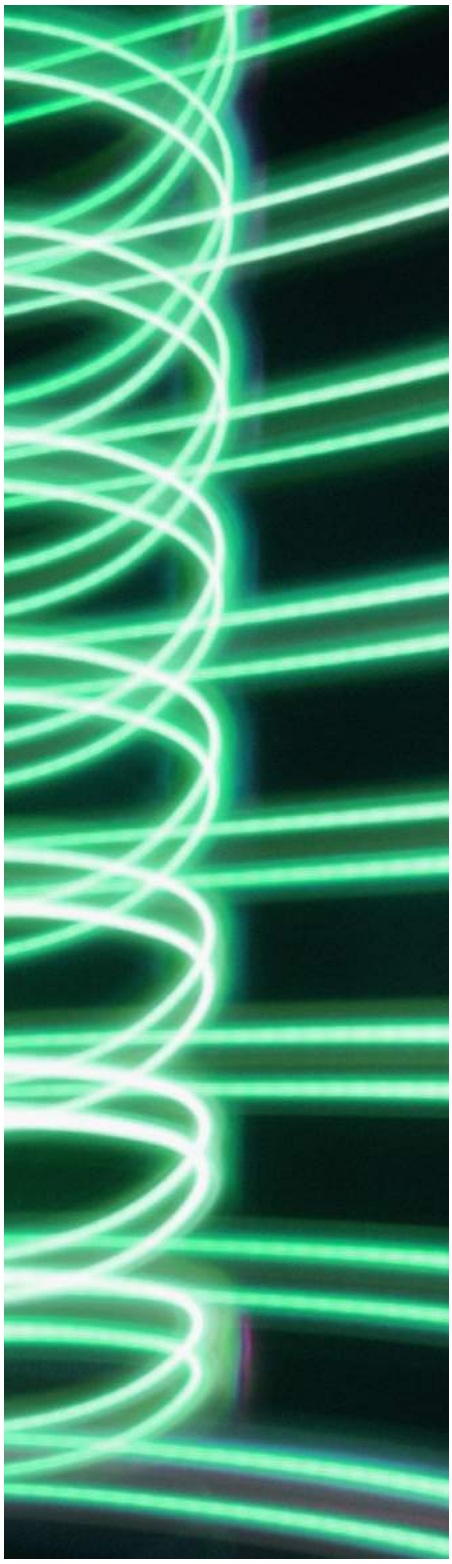
"A lot will depend on case law and regulatory interaction over the next two to five years which will set the benchmarks for this," she says.

Reputational damage

The costs of a data breach are not limited to the legal costs of defending regulatory and legal actions, and the fines and compensation paid out when such actions are lost. There is also the reputational damage to consider. This can be serious, albeit impossible to quantify. It includes loss of brand value, loss of customer trust, reduced revenues and profits and a falling share price.

The cost of the damage will vary depending on the organisation, the elasticity of supply and demand, and customer relationships. If, for example, a bank suffers a major data breach but it has a strong brand, provides excellent services that are difficult for other banks to match and it has built up high levels of customer trust and loyalty, then the reputational damage is unlikely to prove costly. If, on the other hand, it is a bank that is weak in these key areas, then the reputational damage can be much more financially damaging.

Customer trust was an important feature of Deloitte's 2018 survey GDPR six months on, in the questions asked of both organisations and consumers. In their responses, 25% of consumers – in all sectors, not just financial services – said their trust in an organisation would decrease if it suffered a data compromise, and 17% said they would stop using its services or buying its products.



4. Impact on business operations and commercial success

It is one thing to comply with GDPR and avoid, or at least minimise, all the risks highlighted in the previous chapters. It is quite a different thing to ensure that data protection measures do not become so restrictive that they seriously impede the operational effectiveness and revenue generating capabilities of the business.

Such obstacles can be less of a problem for financial institutions than for other types of businesses. Many banks, insurers and investment managers only target consumers who are more likely to want to buy their services, which means those services are more demand-led, so the return on investment in marketing is already quite high.

By contrast, advertising technology companies, direct marketing companies and others target consumers who are more likely to have to be sold services and products. Their services tend to be more supply-led, so direct marketing is a big cost that produces a relatively low return. In addition, financial services firms have largely included *"privacy by design"* principles in their data collection, processing, storage, analysis, and usage. Adjusting to GDPR therefore created little or no impediment to their data-related business operations.

The European Banking Federation says that some banks are concerned that tough rules on the use of AI for data processing could have a negative impact on business operations. Article 22 of GDPR sets out rules to protect people from automated decision-making that has no human involvement. Such decision-making and profiling is allowed, but only under certain circumstances.

"We are mainly of the opinion that GDPR provides a sound and appropriate framework for safeguarding the privacy rights of consumers by ensuring they are not subject to unfair automated decision making," says the EBF's **Hélène Benoist**.

The federation believes, however, that a too strict interpretation of Article 22 could risk hindering innovation.

Simon McDougall of the ICO makes the point that there is much about GDPR that can actually provide a commercial advantage and assist, rather than hold back, commercial success. Instead of viewing the data portability requirement, for instance, as purely a compliance burden, it should be seen as a business opportunity, a way of winning business from competitors.

"Data portability is a double-edged sword," he says. *"Firms have a choice. They can ignore it, and let their competitors use it to their advantage. Or they can use it to win market share rather than lose market share."*

He accepts that any new rules run the risk of having a negative impact on operations and ultimately on profit, and GDPR is no exception. Tensions can develop in a business between the marketing department, which sometimes wants to contact as many people as possible, and the risk and compliance departments, which have to check that what the marketing people are doing is legal.

"But these can be seen as 'healthy' tensions," he says.

"They are promoting the right kind of conversations and sometimes saving organisations from themselves. The more sophisticated marketeers moved on many years ago, to be fair, from contacting large numbers of people then, to now looking for quality leads and conversations that generate trust, and then revenue. The gap between marketing and compliance is much smaller than people originally envisaged before GDPR came in."

BNY Mellon's **Kirsten Mycroft's** view is that GDPR has had a big impact on the operations of retail focused banks that engage in a lot of direct to consumer marketing and associated analysis.

"It may have affected what they can and cannot do in the marketing space, or how they have had to reach out to consumers to gain their consent for certain activities or to confirm their marketing preferences," she says.

"In fact, it has offered the opportunity to engage with clients and give them the assurance that banks have privacy programmes in place. We had enquiries from clients wanting to know what we were doing to comply with GDPR. They cared about it. Like with any of our compliance programmes, while they are intended to meet the requirements of a regulation they are also very much driven by the need for us to maintain client trust and to meet our clients' and employees' expectations. It's not just a tick-box exercise. It has to be truly client centric."

"There is no getting away from the fact that a business that is trying to move in an agile, innovative way finds regulation frustrating," says **Suzanne Rodway**, Head of Legal Operations and DPO, RBS. *"But that doesn't mean it should not do it. When you break down most of the GDPR's requirements they are really good sensible things. There are less sensible rules like those on cross-border data transfers, which in no way help anybody, as they still rely on the idea that a set of data is sent from point A to point B and lead to legal instruments like contracts and BCRs, which don't of themselves protect the data of individuals in the way that the other requirements do."*

"But rules that make businesses think carefully about the data they ask for, what they do with it, who they share it with and that it can only be used if certain legal conditions are met, are all fundamentally good business practices that should be built into processes anyway."

Compliance with GDPR is not always a black and white issue, which gives organisations some scope to be flexible in how they apply it so as not to unduly affect business efficiency.

"GDPR has a lot of grey area, and how we process data is largely open to how we interpret the rules," says the data protection officer of the British subsidiary of one of Asia's biggest banks.

"We will comply with GDPR to a point where it is not limiting the business. Or we will find an operational procedure that will both comply with GDPR in a grey area, and yet allow the business to function."

5. Executive management and board scrutiny

Executive managements and supervisory boards in the financial sector tend to be better at monitoring their data protection policies and GDPR compliance procedures than their counterparts in other industries. This is because their organisations have evolved over decades to meet the strict requirements of a heavily regulated sector, where huge fines can be imposed on those that transgress.

In the UK, the introduction by the Financial Conduct Authority of the Senior Manager's Regime – for banks and certain investment firms in 2016 and other financial institutions in December 2018 and December 2019 – focused minds even more. The regime makes senior managers and directors individually more responsible and accountable for their actions, including compliance with all applicable laws and regulations.

Every senior manager needs to have a "statement of responsibilities" that clearly says what they are responsible and accountable for, some of which are prescribed. At least once a year firms need to certify that their senior managers are suitable for their jobs.

When GDPR came in to force, it added yet another layer of responsibility and risk for senior managers in the UK financial services industry, and consequently reviews and internal audits to keep tabs on things. The most advanced companies have created dashboards and metrics for business leaders. At the moment they are operating in a business-as-usual environment. It is possible they have developed a false sense of security, believing they are doing everything right, because the regulators have not become active. We are probably in the archetypal lull before the storm.

When breaches start happening, the regulators take notice and class actions start flowing, that will be the real test of whether executive managers have been in full control and whether board directors can demonstrate they have been able to provide high-quality, independent oversight and constructive challenge to the executive.

The ICO's Simon McDougall has concerns about how the executive management and boards of financial firms understand their data protection compliance obligations.

"People's understanding of GDPR compliance is often simplistic, and that includes boards and senior management sometimes," he says.

"Some think it is all focused on security, or focused on consent or that it's a restrictive piece of regulation with no upside."

"The good news though is that the GDPR cuts through to the top levels in a way not many regulations do. It was a talking point for a long time and got senior management and boards in virtually every organisation genuinely engaged. They would have had to have been living under a rock to not recognise GDPR as a major issue last year. In that respect, job done."

"The ICO put out a series of myth-busting blogs which was one of the most successful pieces of communications we have done. We have to keep educating everyone, including senior management in financial institutions, about what GDPR actually is, as opposed to what they might think it is from some headlines they have read ."

RBS's **Suzanne Rodway** says her bank's executive management team and board could not be more closely engaged in understanding and ensuring GDPR compliance. She reports directly to the general counsel who sits on the executive management, and reports regularly to the board's risk committee.

"The board have been really interested and have asked in-depth questions," she says.

"They are very aware of the requirements. A lot of our non-executive directors sit on boards of companies in other sectors, so they see the impact of GDPR there."

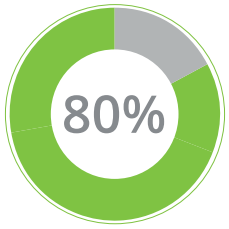
"GDPR is not a huge risk for the bank because we are mainly a B2B bank, so I don't think the board and executive committee are paying excessive attention to it," says the data protection officer of the British subsidiary of one of Asia's biggest banks.

"Their mind-set has been changed, though. Our head office has been deploying a GDPR programme to ensure compliance not only in the overseas subsidiaries and branches, but also in head office as a lot of data is transferred there for processing."

6. Consumer awareness

There is no doubt that financial services consumers are much more aware of their data rights under GDPR than they were under the previous EU rules that had existed since 1995, and under national rules.

Deloitte's November 2018 GDPR six months on report showed that across all industry sectors, not just financial services, 80% of individuals surveyed were aware of the key rights they have under the regulation. They know about the right to receive clear and understandable information about who is processing their data, what data they are processing and why; the right to request access to the data an organisation has on them; the right to be forgotten, to ask for their data to be deleted if there is no reason for a company to keep it; the right to be informed without delay if their data is lost or stolen; and more.



of individuals surveyed were aware of the key rights they have under the regulation

Many financial services companies saw a slight increase in *"data subject access requests"* (DSARs) after 25 May 2018, a data subject being the legal term for a person whose personal data is being held. Activity has since declined as the novelty has worn off. However, there could be a big increase in DSARs if there is a major data protection scandal. Consumers would be assisted by law firms and claims management companies rushing to act on their behalf, just as they did in the UK's long-running Payment Protection Insurance (PPI) mis-selling case.

In the seventh question of our 2018 survey, financial services sector respondents were asked "How has the volume of data requests changed since GDPR came into effect?"

They were asked to rate four different types of request: access, portability, erasure and marketing opt-out. Taking just the first type, data subject access request (DSAR), 65% of respondents working for financial services firms in the seven EU countries covered in the survey said the volume had increased. Looking at the answers given by the all-sector respondents, 60% said the volume of DSARs had increased.

One might have expected the all-sector response to have been a lot higher, representing pent-up demand from newly educated consumers being released. Yet financial sector consumers have filed slightly more DSARs, despite generally being more aware of their access rights because of the long history of consumer and regulatory scrutiny in that sector – clearly there is still a lot of repressed demand.

Noémie Papp of the European Banking Federation believes financial services consumers are generally aware of GDPR and appreciate the rights and benefits it confers on them. *"It has helped and will help them trust banks more,"* she says.

However, some consumers in certain cases misunderstand the rights GDPR gives them. They may know that the regulation allows them to withdraw their consent from banks to process their data, but do not realise that in certain cases *"consent"* is not the only legal ground for processing personal data.

"Banks are having to explain to these customers that they can still process their data without their consent in order to comply, for example, with anti-money laundering and know-your-customer requirements," says the EBF's Hélène Benoist. "Many consumers have misunderstood this and still need to be educated about their rights under GDPR."

Martin Collins, Chief Privacy Officer of Invesco sheds some light on his firm's experience in this respect: *"Pre-GDPR, there was a lot of noise in the market about a predicted increase in the number of DSARs. Whilst we received an increase in DSARs since GDPR came into effect, the increase is not nearly as much as was anticipated. Initially, we experienced an increase in right to erasure requests from former customers who believed GDPR provided a right to have their personal data erased as soon as they closed an account. In response we had to raise awareness that other regulatory rules in financial services, such as AML, require this data to be retained for five-plus years after account closure."*

"We also observed a slight increase in 'No-win, No-fee' litigation or claims firms trying to use DSARs as a tool. It has become easier for litigation firms to try to experiment with DSARs, particularly since the £10 fee, which acted as a barrier in some regard, was removed. There has also been a trend for unsuccessful job applicants to submit DSARs for all information relevant to decisions on their application. DSARs involving searches of communications data, such as email or instant messaging, are by far the most complex and resource intensive to address."

Consumers of financial services are broadly more cognisant of the greater protection GDPR gives them according to ICO research. *"Complaints to us have more than doubled year on year, which is indicative of stronger public awareness and engagement,"* says **Simon McDougall**, Executive Director, Technology Policy and Innovation at the ICO.

"Financial institutions are also seeing more engagement from their customers about this. At the same time, we still think more needs to be done to explain GDPR to customers and to improve general digital literacy. There is still a lot of mistrust of new technology and innovation. That mistrust will hamper innovation if people chose not to engage with the clever technology out there."

The financial services sector has always had customers who have been quick to complain if they are not happy, says **Suzanne Rodway**, Head of Legal Operations and DPO at RBS.

"That's why we haven't seen a massive increase in subject access requests. We already get far more than any other industry. But we have had a few more people writing in who want to be forgotten or to exercise other rights."

7. Recruiting specialist staff and training non-specialist staff

GDPR has created such an unprecedented demand for specialist staff that many companies have struggled to meet their recruitment targets. The largest have had to take on data protection officers, data privacy managers, and other senior GDPR-focused staff to play dedicated roles. Whilst smaller firms have not needed to create specific roles, they have needed to allocate the responsibilities of data protection to a specified legal or compliance expert to take on these responsibilities as part of a wider role.

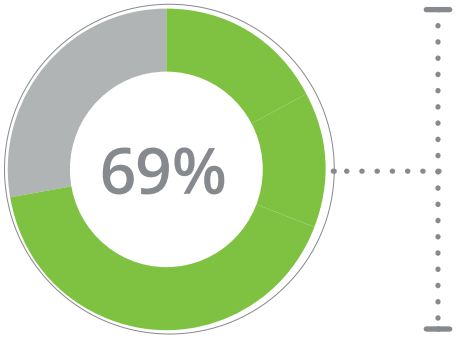
Banks, investment managers and other financial firms with larger financial resources than most firms in other sectors, and therefore the ability to offer attractive salaries and employment conditions, have found it easier to take on senior data protection professionals. However, for the next tiers down – middle ranking and junior positions – it has been more difficult. This is because the talent pool of people who understand privacy by design principles and data protection compliance is small. People in those lower reaches have been snapped up by organisations for senior roles, leaving the pool depleted so that even global banks dangling enticing bait have been left with small catches.

In the third question of our 2018 survey, respondents were asked "Has your internal GDPR-related headcount changed over the last two years?"

Some 47% of respondents working for financial services firms in the seven EU countries covered in the survey said there had been an increase. By contrast, 69% of all-sector respondents said there had been an increase. This wide disparity in responses can be attributed to the fact that financial institutions have for many years had to comply with strict data protection regulations, and so have built up considerable in-house expertise, whereas companies in other industry sectors have faced less strict requirements and have smaller internal resources.

The European Banking Federation's Hélène Benoist says it is true the banking sector is generally perceived as being able to pay higher salaries than other sectors and so can buy the best expertise on the market, though not in every instance.

"It is also true that because of a long tradition of looking after customer data, and because many European countries already operated strict data protection laws, a lot of in-house knowledge had built up in banks so they can rely on such expertise within the organisation," she says.



of respondents working for financial services firms in the seven EU countries covered in the survey said there had been an increase

Non-specialists

As for staff who are not data protection specialists who work outside the data management, legal and compliance departments (such as customer relationship managers, marketing managers, sales managers and telesales operatives), they have had to be trained in the basics of GDPR compliance and regularly reminded about the procedures and guidelines to follow.

Privacy professionals in financial firms have got better at communicating to staff what privacy means and why its important, but it is not perfect. There is often a gap between what the professionals understand about the subject and complying with data protection rules, and what frontline, customer-facing employees understand.

Financial institutions generally had well-resourced training programmes for all kinds of legal and regulatory compliance requirements, including data protection. They know how to train staff, and then test, evaluate and monitor its effectiveness. All they had to do in preparation for GDPR was to update and expand existing training initiatives.

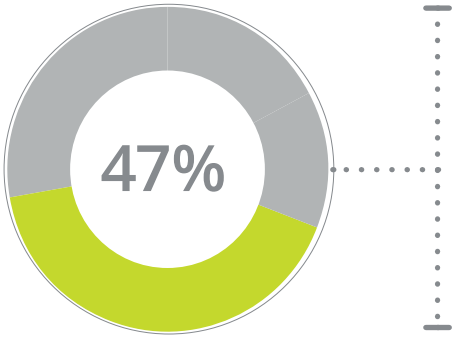
"There is a limited pool of really experienced people, those who have not just gained a certificate or worked on a GDPR programme, but who have the practical experience of applying privacy rules to a wide variety of scenarios on a day-to-day basis," says **Kirsten Mycroft**, Global Chief Privacy Officer at BNY Mellon.

"That is very different from being able to quote what the law says. You need to be aggressive in terms of recruiting qualified individuals."

Some data protection departments are struggling to keep staff fully appraised of their duties under GDPR.

"We rely on our staff to understand our data protection policies, but because we are so busy doing our day-to-day jobs I don't think the right training has been provided to the right people in every case," says the data protection officer of a British subsidiary of one of Asia's biggest banks.

"Knowing where personal data is and what we are doing with it can be difficult. The business people who know where it is and are using it may not be paying enough attention to privacy, and therefore may not be telling the privacy people all they should be telling them."



of respondents working for financial services firms in the seven EU countries covered in the survey said there had been an increase

8. Technology-assisted GDPR compliance

Technology plays an important role in protecting data. Data Protection Impact Assessments (DPIA), which help companies identify and minimise data protection risks, are an integral part of a privacy by design approach.

A large number of solution vendors – long-established ones and start-ups – offer online and offline DPIA tools that can be tailored to each company's requirements to provide compliance monitoring and oversight, ensuring all processes are adhered to. Other solutions are available for data inventory management, unstructured data scanning, cookie compliance, data subject access requests and consent management.

These solutions are not always used as well as they should be by financial institutions. There has been a proliferation of new offerings from existing vendors and new entrants, spending a great deal of money on marketing, which can be confusing. Users need to be clear about the value they hope to get from them before committing.

In the 11th question of our 2018 survey, respondents were asked "Have you invested in tools and technology in the following areas to support your compliance activities?"

The eight areas are shown below, along with the responses from financial services respondents (first column) and all-sector respondents (second column) in the seven EU countries surveyed. Those answering "Yes," they are using internally or externally developed technology tools, are as follows:

Area of technology invested in	FS sector	All sectors
"Article 30" inventory management	72%	71%
Data Protection Impact Assessment (DPIA) execution	68%	70%
Unstructured data scanning	80%	69%
Cookie compliance	79%	76%
Subject access request discovery	76%	75%
Governance, risk & compliance	80%	72%
Data loss prevention	79%	77%
Consent/preference management	72%	73%

The results show that technology is a major enabler when it comes to GDPR compliance, in all sectors not just financial services.

Simon McDougall of the ICO believes firms still have much to do on the technology front.

"What we haven't seen much of, until now, is integrating GDPR into the technology side of the organisation," says the ICO's **Simon McDougall**.

"In many cases the technology has not been brought up to date, and there are still a lot of manual rather than automated controls."

"Our use of technology will increase," says **Kirsten Mycroft**, Global Chief Privacy Officer, BNY Mellon.

"We are automating some of the processes that were manual for day one GDPR compliance."

Some banks admit to not using any form of sophisticated technology to ensure data protection compliance.

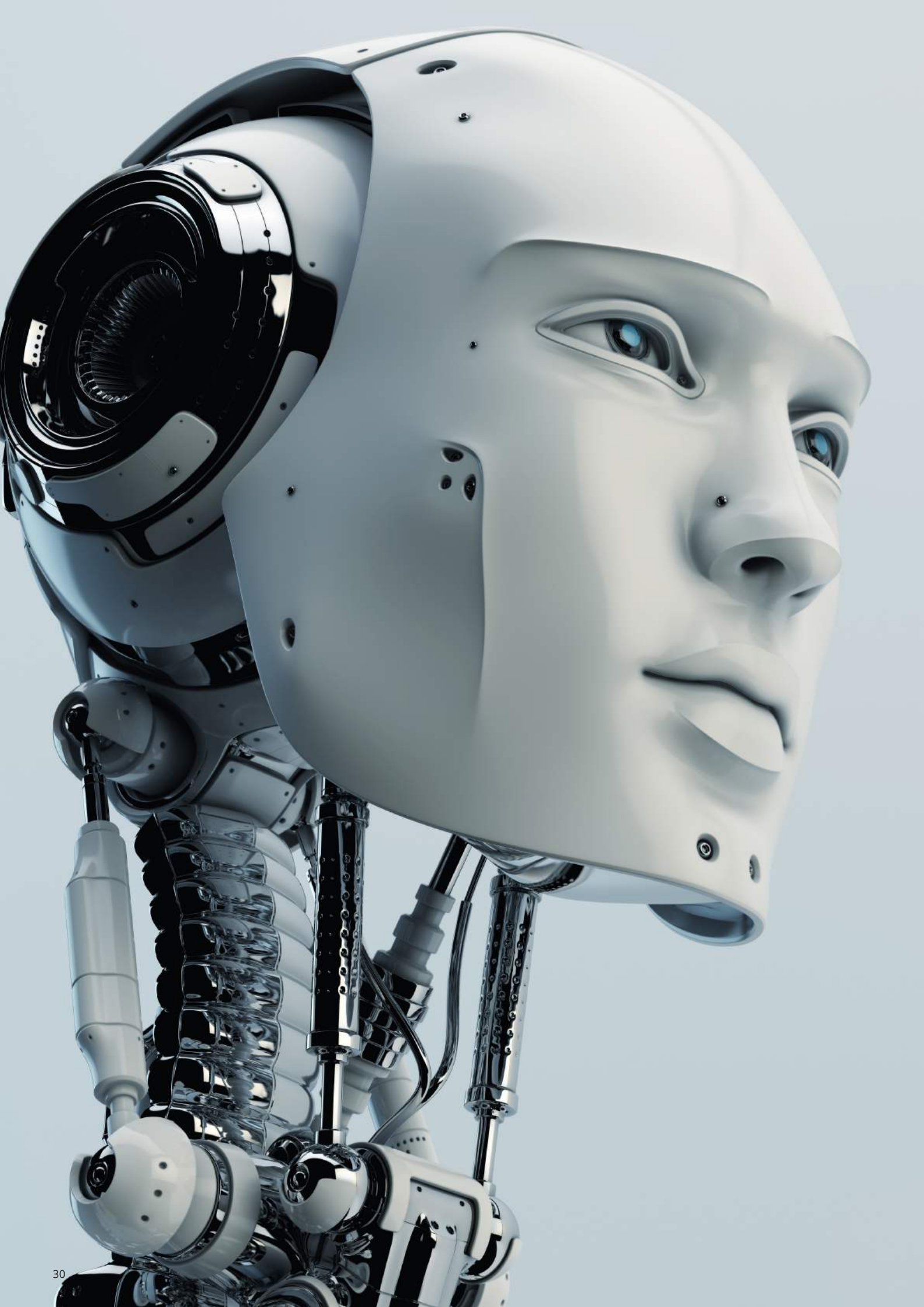
"We use technology to scan emails for spam and malicious executables, but not for personal data," says the data protection officer of a British subsidiary of one of Asia's biggest banks.

"Most data received through emails is unstructured so it is hard to find a DLP (data loss prevention) solution that will work. But if I get my way, we will be implementing a DLP solution to identify personal and other types of data, classify it and protecting those information assets correctly."

Suzanne Rodway, Head of Legal Operations and DPO at RBS, says technology-based tools are used, but they are internal ones. They are not brought-in from outside.

"One of the things that annoyed me most about GDPR was how many solutions vendors came out of nowhere saying they could make us GDPR compliant," she says.

"It is not one single thing for which a single solution can be found, it is hundreds of little bits of pieces. We own the technology-based tools we use and have repurposed these internal tools for breach management, DPIAs and DSARs reporting."



Artificial intelligence – analysing data in an ethical and compliant way

Artificial intelligence is increasingly used by organisations to analyse data, and there is no doubt about its benefits, but it should be used ethically. It should not include any biases – conscious or unconscious – against people because of their race, religion, sexual orientation or certain other characteristics. The European Data Protection Supervisor notes that the ability of computers using AI algorithms "to analyse huge data sets and make predictions…presents challenges for privacy and data protection."

Organisations using AI in any significant way should therefore set up a robust governance structure to ensure it is used ethically, but how to do so is taxing the cleverest business, technological and legal minds. The British government set up a Centre for Data Ethics and Innovation in late 2018 to look into this. Its purpose is to advise organisations and regulators on the ethical use of data in all areas of the economy and society, and the technologies that collect, process, analyse and store it. Its role is to advise, not regulate – regulatory and supervisory roles will remain with the ICO and industry regulators.

The centre will help "deal with the novel ethical issues raised by rapidly developing technologies such as artificial intelligence" and other "data-driven technologies", said Matt Hancock, Secretary of State for Digital, Culture, Media and Sport, at the centre's launch. The centre could "lead the global debate on these vital and far-reaching issues".

The consultation document on how the centre will function gives examples of the ethical issues raised by the use of AI to process data: it can gain powerful insights into human behaviour which could be used to influence people's decisions without them realising; it could be used to reject job applications without a clear explanation; or it could be used to stifle competition and innovation from new entrants to a particular market.

The centre's 2019/20 work programme includes a review of how data is used to shape people's online environments via the personalisation and targeting of messages, content and services. It also includes an investigation into algorithmic bias in various sectors including local government, justice, recruitment and financial services. Such bias can have a significant negative impact on people's lives, and there is a risk of algorithms "worsening biased decision making", says the centre.

Financial services is therefore a priority area where the ethics of AI must be addressed. It will be interesting to see how this is done, but it certainly will not be easy.

9. Has it all been worth it? And what's next?

Now the dust has settled we know a lot more about the compliance burden GDPR has placed on financial firms. It has taken a great deal of management time, financial investment and re-engineering of policies, procedures and technology processes to arrive at the current, high-level state of compliance.

Financial regulators, like regulators in any industry, like to conduct cost-benefit analyses for their new rule-making. Balancing the costs and risks that GDPR has placed on financial services firms, against the benefits that have accrued to their customers, to what extent has it been worth it for both parties?

Simon McDougall of the UK's ICO believes the compliance costs of GDPR are far outweighed by the benefits for financial firms and their customers.

"GDPR was an incredibly ambitious piece of legislation. Its objective was to re-write how the handling of personal data is regulated in Europe. When you think how much information is personalised now, and how every firm is a data firm, it was an incredible thing to attempt in one go, but it succeeded."

"Most financial organisations are comfortable with the individual elements of the regulation. Data portability, good. The right to be forgotten, good. These things are novel and challenging, but firms are not saying they should not exist."

Kirsten Mycroft, BNY Mellon's Global Chief Privacy Officer, believes that GDPR compliance helps maintain reputation and trust.

"Your clients expect you to do it. Your employees expect you to do it, and to get it right. Recent breaches have brought it into sharp focus and show that there is a need for smart regulation in this area", she says.

"It will benefit society as a whole because it holds organisations to account, will help to prevent future data misuses and will increase transparency. Consumers will have a better understanding of what their personal data is being used for and by whom. As a society, we should continue to carefully manage the balance between responsible regulation, our ability to keep pace with technology advancements and our continued ability to innovate."

What's next

Looking ahead, what more needs to be done to maintain compliance with GDPR, and prepare for similar rules being introduced around the world? *"Privacy by design,"* or *"data protection by design"* as it is referred to in GDPR, is the answer.

The European Commission describes it as this: Companies [and other] organisations are encouraged to implement technical and organisational measures, at the earliest stages of the design of the processing operations, in such a way that safeguards privacy and data protection principles right from the start ('data protection by design'). It gives two examples:

- The use of pseudonymisation – replacing personally identifiable material with artificial identifiers.

- The use of encryption – encoding messages so only those authorised can read them.

The UK's Information Commissioner's Office puts it like this: *"In essence, this means you have to integrate or 'bake in' data protection into your processing activities and business practices, from the design stage right through the lifecycle. GDPR should not be a 'tick-box' exercise. Data protection by design is about considering data protection and privacy issues upfront in everything you do. It can help you ensure that you comply with the GDPR's fundamental principles and requirements, and forms part of the focus on accountability."*

The concept is not new. It has always been an aspect of data protection procedures, but under GDPR is now a legal requirement.

Organisations fully accept this. *"We need to ensure sustainable compliance and weave it into the fabric, into the DNA of the organisation,"* says **Kirsten Mycroft**, Global Chief Privacy Officer, BNY Mellon.

"The other thing I'd call out is the need to join the dots across the various data disciplines within the enterprise. Very often there are different silos for data security, including data governance, data quality, and records management, etc and to get privacy right you need to be collaborating across all those data disciplines, as well as with the business lines, technology, risk, and compliance."

"You cannot throw a set of instructions or a policy over the wall to the business. You have to give them the tools and support to comply. You have to look at your operating model, make sure it enables compliance and weave privacy into the DNA of the company. It is privacy by design and 'privacy engineering', right from the outset. You have to make it part of the way you work, part of day-to-day practices."

Some compliance experts believe a gulf could open up between what data protection departments will strive for and what business leaders will be prepared to give them.

"Privacy professionals will want to drive for further improvements, but top management may think differently because of the cost and impact on business efficiency," says the data protection officer of a British subsidiary of one of Asia's biggest banks.

"The fact that there hasn't been a lot of action by the regulators so far, and that they haven't looked at the big banks' privacy practices to see if they are complying, means the fear has gone away among some bank executive management. They may say to privacy professionals, 'you can ask for further improvements, but we are taking a risk-based approach and the risks are pretty low right now, so we will not provide the budget'."

"I don't think there will be further enhancements to data protection until a big data breach hits the headlines and a company receives a big fine. The danger is, a lot of banks think they have complied with GDPR, and that's it. Yet they should continue to try to improve rather than accept the status quo. If you have a retail arm you will probably continue to spend money on improving your processes and technologies. But if you are a corporate bank you will be more likely to take a risk-based approach."

He believes we are in a kind of *"phoney-war"* situation, where there has not been much conflict between financial services companies on one side and consumers on the other. That could change at any time.

"Right now, consumers are not that aware of GDPR, which they have to be if they want to get back at a company they think has treated them badly," he says.

"As people do become more aware, more will take action and report alleged compliance failures to the regulator. Such efforts will only be effective, though, if the data protection authorities are staffed-up well enough to deal with a big increase in complaints."

Suzanne Rodway, Head of Legal Operations and DPO, RBS, says the next big step is to prepare for similar data protection regulations being introduced in other countries. The task should be relatively straightforward considering the experience gained in the last few years.

"Getting the European side right is the main thing, but we track what is happening in other parts of the world," she says. We are in Singapore and Hong Kong and they have privacy regulations. "We are in India, and there is a significant draft law on the table there. It is only a matter of time before there is a federal privacy law tabled in the US. However, if you have got yourself into a decent state from a European perspective, then as these other laws come in it should only need little tweaks on top for local differences."

It is clear that *"data protection by design"* is the ideal approach, and should deliver the high level of compliance organisations require. Even so, there is no such thing as a perfect state of compliance. As rules change, organisations have to adapt. They have to be alive to how their organisation works and ensure that data protection, legal and compliance managers are closely aligned with the business managers, and that these various groups adapt and move with each other, constantly. In regulatory compliance, only one thing is certain – the job is never finished.

Contacts

Maya Goethals
Senior Manager
mgoethals@deloitte.co.uk

Stephen Bonner
Partner
stephenbonner@deloitte.co.uk

Peter Gooch
Partner
pgooch@deloitte.co.uk

Report Authors

Maya Goethals

Michael Imeson

Contacts Luxembourg

Roland Bastin
Partner - Risk Advisory
rbastin@deloitte.lu
+352 451 452 213

Jean-Pierre Maissin
Partner - EMEA FSI Analytics Leader
jpmaissin@deloitte.lu
+352 451 452 834

Irina Gabriela Hedea
Partner - Risk Advisory
ighedea@deloitte.lu
+352 451 452 944

Georges Wantz
Managing Director - Technology & Enterprise
gwantz@deloitte.lu
+352 451 454 363

Acknowledgements

We are grateful to the Deloitte Cyber team

Stephen Bonner, Peter Gooch, Andrew Johnson, Nick Seaver, Rajee Sritharan and Victoria Olley for their insight and guidance, without which this report would not have been possible.

Deloitte.

Designed and produced by Deloitte CoRe Creative Services, Rzeszów, 258362