Executive Brief

Data Governance, Customer-Centricity, and the GDPR

Sponsored by: Informatica and Cognizant

Lawrence Freeborn
July 2016

THE IDC POSITION

IDC believes that the number one priority of any financial services institution should be customer-centricity.

Ultimately, how well a financial services institution can serve its customer comes down to how well it manages its data, and how well it exploits it.

Eventually, therefore, data governance will be seen primarily as a way of supporting and enhancing the customer experience, with customer experience on a par with regulatory compliance as the main driver of data governance.

The financial services industry is not at that stage yet: but the multi-year push to achieve BCBS 239 and SOLVENCY II compliance brings that stage closer, since they can be viewed as a set of data governance best practices.

And the next focus for data governance is compliance with the European General Data Protection Regulation (GDPR), which was adopted by the EU in April 2016.

Ideally, financial services institutions should not simply think about GDPR as a compliance exercise, but how they can best ensure world-class customer service in the light of it. These are the two sides of the overall data governance challenge.

Overview of the GDPR

The General Data Protection Regulation is considerably more than an attempt to harmonize data protection laws across Europe. As much as in any area of regulation, it reflects an effort by the European Union to lead the conversation on the subject of data protection and data privacy. The stated aim goes beyond harmonization and talks of GDPR as an "Essential step to strengthen citizens' fundamental rights in the digital age."

As such, the EU is shaping up to implement a strict data privacy regime, with far-reaching implications for customer service and a huge amount of preparatory work in terms of compliance (see below). Underpinning the GDPR is the idea that information around personal identity should be viewed as an asset like any other. It therefore deserves the same protection as any other type of asset, with all that this entails for processes, controls and protections.

The GDPR is not specific to the financial services industry, but covers the controllers (the firms which own the customer relationship – so banks or insurers) and processors (in the case of the financial industry, the banks and insurers' technology partners which handle customer data on their behalf) of all data relating to citizens of the EU in every industry; i.e., almost everybody. But as the custodians of huge volumes of valuable and personal data, financial services institutions stand to be some of the most affected of all industries.

Financial services institutions will be leaving themselves open to enormous fines if they fail to adhere. The penalty for non-compliance will be up to 4% of global annual turnover or €20 million, whichever figure is higher. This alone should be enough for all financial services institutions to take note, prioritize the GDPR and start preparing without delay. They have until May 2018 to comply, so they should start preparing without delay.

Major Rights

The GDPR will bring in the requirement to confirm explicit and unambiguous consent from customers about what a financial services institution wants to do with their data. The consent will have to be time bound, so data can't be used indefinitely, and it will have to be specific. A Data Protection Officer (DPO) must be designated in every public body and company where large-scale data monitoring takes place. And the concept of pseudonymization is proposed, whereby data is processed in such a way that it can't be traced back to the individual without more data added to it, so reducing the risk of private data being misused in the event of a breach.

There are also a number of rights that are enshrined in GDPR, including the right to object to data processing, whereby the financial services institution would have to demonstrate to the subject that processing must continue for legal or other reasons, the right to rectify data, and the qualified right to bring class actions.

But here are four major rights:

Subject Access Request

Individuals will be able to request details of what information is held on them by data controllers, which typically have a month to respond but can in complex cases take an extra two. The details that need to be provided include a copy of the data itself, an explanation of how the data is used, which types of third parties also have access to it, and how long the data is or needs to be stored for.

> "You could potentially have to go into every single system and get every piece of customer data. That would be big, but if it is a case of reporting back to the client a business summary of what has been accomplished, we are already doing that."
>
> **Switzerland-based GSIB**

Data Portability

This allows individuals to request that their data profile, or the data held on them by a data processor, be passed to another processor on request. In practical terms, the GDPR data portability terms allow financial services institutions to compete on equal terms with incumbents for an individual's custom, as another financial services institution could perform the same types of analytics as the incumbent with a view to personalizing service.

Notification of Breach

Data breaches need to be reported to the regulator within 72 hours and the subjects of the breach need to be notified as well. If processors can demonstrate that the data is encrypted, or there is a low risk of damage, they may be able to get away with notifying the supervisory authority rather making a public announcement or contacting each subject individually.

Right to be Forgotten

The Right to be Forgotten has been popularized by the compliance of search engines such as Google, and GDPR applies this across the board. Individuals can require that data be deleted where it is no longer needed, or can withdraw previously granted consent.

Where do Financial Services Institutions Stand?

Understanding

The level of understanding about GDPR across the European financial services industry is mixed, and this has consequences for attitudes and strategies towards it. Even though data privacy itself is an established concept and an established part of regulatory regimes across the continent, there is no consensus on how much work will be required to comply with GDPR. Some financial services institutions believe that it will be relatively straightforward, while others perceive a big new burden.

Many, however, are unfamiliar with GDPR at all, and are only starting to assess the impact. And all these statements apply to those whose business it is to manage data within financial services institutions. The level of awareness outside of the data protection officers and legal teams is generally very low.

Even those financial services institutions that are furthest ahead, and have a program already in place to address GDPR, are still at the information gathering stage, focusing on increasing their understanding while taking legal opinions on the impact.

However, other financial services institutions are already aiming to comply with the minimum of the GDPR allowed, and looking to prioritize which bits will be viewed as most crucial by the regulators and will have the highest impact on individuals. In practice this usually means the notification requirement after breach, since the need for notification is triggered automatically rather than by the customer, and because notification must happen within 72 hours. While the customer initiated parts of GDPR – the subject access request and the right to be forgotten – allow slightly more latitude in how they are approached by the institution, the notification has a hard deadline and will also likely include specification of how exactly the notification should happen.

This position is supported by a belief that the regulators will be pragmatic in enforcement and the application of fines, and that those banks that can demonstrate suitable efforts to meet compliance are likely to be viewed benevolently. The flexibility regulators have shown towards banks on SEPA and BCBS 239 compliance, for example, helps explain some of this complacency.

> "There are rules and regulations we will be able to leverage. But ultimately this is a beast in its own right that we will have to implement."
>
> UK bank

This belief should not prevent financial services institutions looking to improve their data governance and privacy regimes as an end in itself.

One looming unknown is how personal information will end up being defined. Essentially, what is the minimum amount of data that needs to be included in any request? Will a financial services institution be deemed compliant if it provides a summary of data in response to a subject access request, or will it have to draw every piece of data relating to a customer, from every system?

If it is the latter, then getting a total handle on customer data could lead financial services institutions down some long-neglected paths, including to document storage facilities.

Where Financial Services Institutions Are

Financial services institutions in different countries will be starting from different places, and will have had differing data privacy priorities pre-harmonization. They will end up with differing change programs depending on how close GDPR is to their national regulator's existing stance.

Therefore, the best case about what financial services institutions actually need to do to comply is – not too much. The GDPR is designed to harmonize existing privacy regulations which means that, for example, financial services institutions can take the approach of filling in the gaps between their previous national regulation, such as the UK Data Protection Act (DPA), and the GDPR. This means there is still work to be done; but generally it is a case of intensifying current practices rather than anything more fundamental.

For example, subject access requests are already part of the UK's DPA, and so financial services institutions are already used to responding to these. The processes involved are already in place at UK players if not European ones, and the effect of this aspect of GDPR on UK financial services institutions will see them increasing their workforce and spending on fulfilling subject access requests in the short term, and then working out how to speed up the process.

As for the rest of Europe, those banks that have not had to deal with this before will have to get used to the idea of pulling out all relevant data about a particular customer and presenting it to them, within the time restrictions.

The seed of data portability already exists in the UK, in the form of the "Midata" initiative. Midata mandates that banks (and utility providers) adhere to common formats in certain categories of data, meaning that consumers can input this data in price comparison websites.

Similarly, German institutions already have to report data breaches to customers in 72 hours, which is the same standard as GDPR. In the Netherlands, a rule in place since January 2016 requires that data controllers notify the national Data Protection Authority as well as individuals affected of any breach, and notifications are running at more than ten a day in the country.

Meanwhile in France, the government has moved to align its policy with GDPR even before the EU regulation comes into force. This year will see fines for non-compliance increased from a maximum of €300,000 to the GDPR standard of €20 million or 4% of annual global turnover. The right to data portability will also come into force early in France.

But banks in other countries will start from different positions.

However, even within the more advanced countries, some feel that the extent of change required is much more substantial.

This is partly because of the prospect of renegotiating contracts between financial services institutions and their technology partners since the GDPR mandates new liabilities to the processors. Modern business models and outsourcing arrangements mean clarity on this subject is difficult to gain without considerable effort, and it influences not just liability but also what changes need to happen to existing relationships and contracts to minimize risk. This is one reason cited why the compliance process could be drawn out long beyond the 2018 deadline. How this shared liability works out in practice will have to be tested.

The overall effect will be that much more data will need to be documented on a much more granular level. Policies will need to be rewritten and new processes embedded, and this will require plenty of preparation over the next two years.

For those financial institutions that have been pushing forward with their data governance policies already, this process should be a further step in the same direction. Almost none of the industry has been standing still in this area, but many players in the past few years have been engaged in building "data lakes," and deploying Big Data analytics and master data management solutions to extract value from that data. Indeed, making the best use of all that data has been seen as a critical competitive tool as financial services institutions look to personalize their customer experience proposition. With the multiplication of restrictions, consents and expiries on that data, the governance of those data lakes becomes more complicated and even more important.

What Does GDPR Mean for Customer Service?

Individuals are already plenty used to ticking boxes online to accept terms and conditions. They have also grown accustomed to accepting the use of cookies by websites. Granting consent to use their data could become a similar reflex. But it could be the case that frequently being required to give consent – which must now be time limited and for specific purposes – to financial partners to use their data will be seen as a chore. It will not be avoidable in the same way that cookie acceptance is.

> "As customers see banks crossing i's and dotting t's to comply, they could become really annoyed."
> **Large European financial services institution**

Alternatively, individuals could become more selective with their data. There could end up being two tiers of customer, between those that give their consent to their data being used, and those that don't. Those that don't will not see the same level of personalization in future; they could also end up being asked to pay for services in lieu of sharing their data. In this way consumers could start to get a feel for the monetary value of the access they grant to their financial services partners. This would present another data challenge for financial services institutions though, in terms of splitting the customer base into consenting and non-consenting categories.

Meanwhile, the degree of personalization that financial services institutions can offer is likely to be impacted by the restrictions in the GDPR of "profiling," or segmenting the customer base to target marketing messages, particularly when this process is automated. Trying to anticipate customers' needs based on what is known about the customer combined with other datasets has underpinned many of the recent gains both in personalization and advertising, but under GDPR this will become more difficult, with individuals having a right to object.

So, certain avenues could be closed off by GDPR, and financial services institutions will have to re-imagine how they can differentiate themselves, how they can build loyalty in a world where profiling is harder and data is portable.

Where are the Competitive Opportunities for Financial Services Institutions in Relation to GDPR?

The extent to which risk management is involved in discussions around GDPR is also an unknown at present. Since data protection will have the same status as anti-money-laundering and anti-bribery legislation, banks and insurers may be encouraged to look on the issue in a similar way.

Ultimately, questions about the growth of financial services institutions – whether moving into new regions, launching new products or making acquisitions – could come to hinge on the risk associated with customer data.

This should lead to new competitive opportunities for those institutions that have more willingness or more capacity to take on extra (data) risk, or are more efficient at managing it. Similarly, the new liabilities involved in processing data may lead firms to withdraw from certain activities, particularly as the attitude of regulators towards compliance becomes clearer over time, and test cases appear. So GDPR is bound to impact the market for processing customer data, with expertise in the legal contours of the new regulation and robust risk management becoming prized assets.

Most financial services institutions are not yet looking at the GDPR as a competitive opportunity, but this will come. Just as some avenues are closed off by GDPR, others will open up. The

transparency envisaged by the EU may end up being prized by individuals, and those institutions that can best embody the ideal of data transparency and responsibility stand to benefit.

In the first instance, efficiency in compliance will be prized. This goes back to data governance: clear rules for storage of and responsibility for data will save time and effort. Chief Data Officers (CDO) and Data Privacy Officers (DPO) must focus on instilling a data governance culture that prizes the correct labelling and storage of data so that any piece of data can be easily retrieved, deleted or summarized as the need arises. The scope for differentiation will be magnified depending on how the minimum data expectation is set by regulators in different countries.

As individuals exercise their rights more often and the volume of processing required increases, the importance of efficiency will increase.

But the leading financial services institutions – those with the most advanced data governance – will start to think creatively about how to comply, and how best to communicate with individuals as well as other third parties.

> "I fear that with the implementation being rushed, banks will have to develop their own solutions. But if we had common definitions, someone could develop an app that could interrogate the banks easily and extract what information they have."
>
> **Tier one European lender**

For example, the experience of banks in the UK is that interaction with customers can reduce the amount of processing for subject access requests by properly understanding what information the subject is after, and what the minimum amount of information is that will satisfy them. This could involve the application of analytics that allow banks to deal more proactively with subject access requests.

Self-service was identified by IDC as one of the more advanced capabilities financial services institutions could target through their data governance. This could apply in the case of GDPR, if data controllers can use APIs to expose the data which is needed to comply with requests – whether the objective is to access data to present it to the subject, or to delete it – and allow a degree of custom self-service in relation to their data. This could form the basis of innovation in how GDPR is complied with, but it will require confidence on the part of the financial services institution that the correct data is exposed in the correct way.

CONCLUSION: ESSENTIAL GUIDANCE

- Those financial services institutions that are most advanced with their data governance generally will find GDPR easiest to comply with. However, there is plenty of work for all players in the market, and the deadline is close.
- Understanding of the GDPR specifically is lacking, so the first step for many institutions should be to build awareness, initially among key stakeholders but eventually across the firm. The size of penalty for non-compliance should be a call to action in itself.
- There are software solutions available to help with different aspects of GDPR, such as Master Data Management, Data Masking and Data Discovery solutions, which financial services institutions can consider.
- Just like other data governance challenges such as BCBS 239 and SOLVENCY II, compliance with GDPR should be viewed as a reason to strengthen data governance and an opportunity to implement best-in-class practices. Every financial services institution in Europe and beyond will have to comply: but those that do so first, best and cheapest will be at an advantage, and will be able to think creatively about how to integrate GDPR compliance into their customer service proposition.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.620.5533
Twitter: @IDC
idc-insights-community.com
www.idc.com