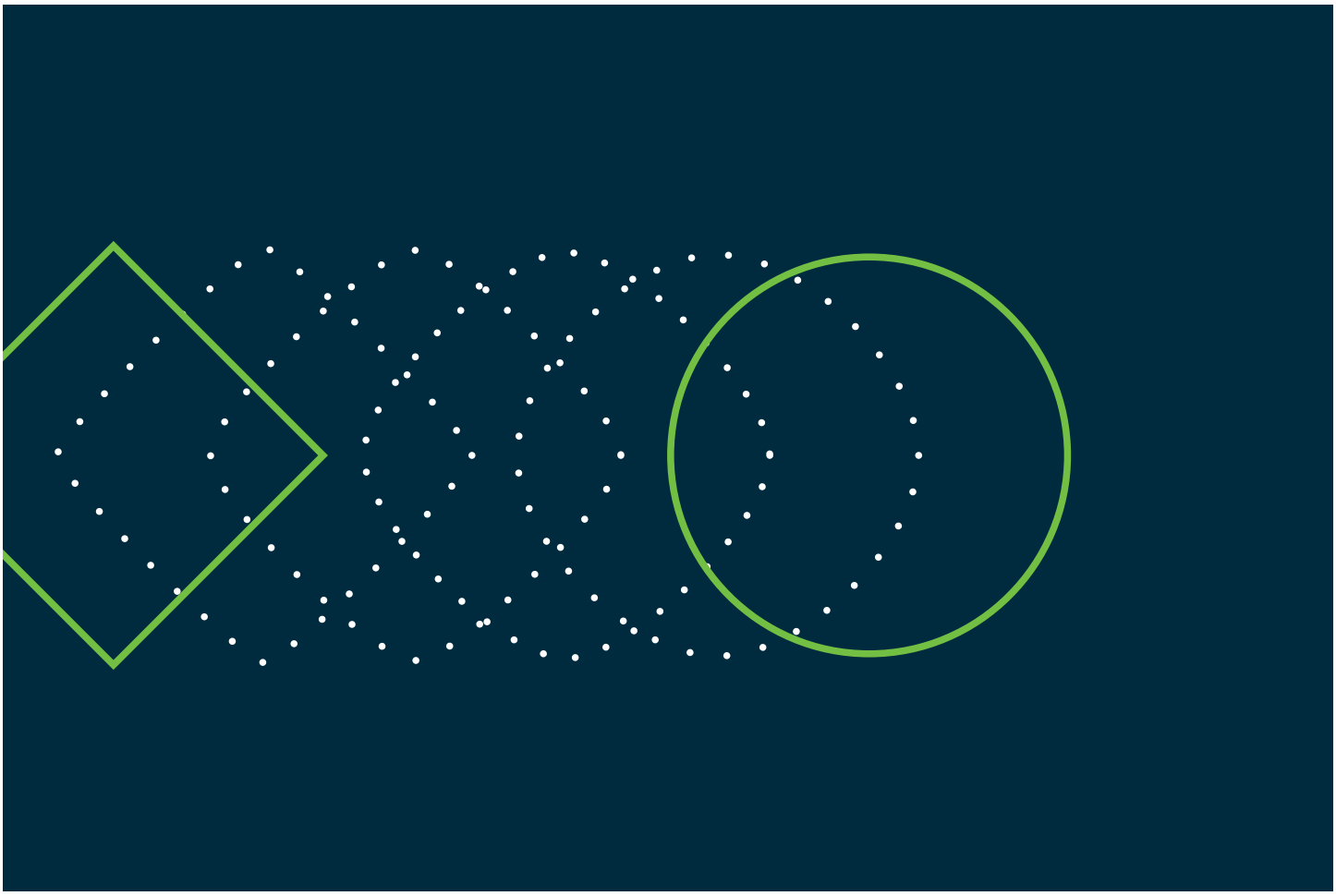
Collibra

Whitepaper

How to think strategically about digital transformation and data privacy in financial services



Introduction

Traditional financial services firms around the globe — banks, insurers and asset managers — need to embrace both digital transformation and data privacy simultaneously to thrive in the coming decade. These two objectives are deeply intertwined because the success of digital transformation programs is highly dependent on an organization's ability to engage with personal data, including data privacy compliance and ethics issues.

48% of financial services organizations have embedded fintech fully into their strategic operating model and 94% are confident that fintech will support their organization to deliver revenue growth over the next two years.

Many financial services firms are rushing to adopt more technologically sophisticated approaches to fostering and sustaining customer relationships. According to a recent PWC survey, 48% of financial services organizations have embedded fintech fully into their strategic operating model and 94% are confident that fintech will support their organization to deliver revenue growth over the next two years. More than half of the financial services executives polled assert that emerging technologies and artificial intelligence (AI) will transform the way companies deliver products over the next two years. The report declares, "Sharp use of AI, IoT and big data is critical in creating the necessary customer insight and agility to meet demands. It's also a matter of culture; firms need to embrace data-driven decision making and move from product push to customer pull."

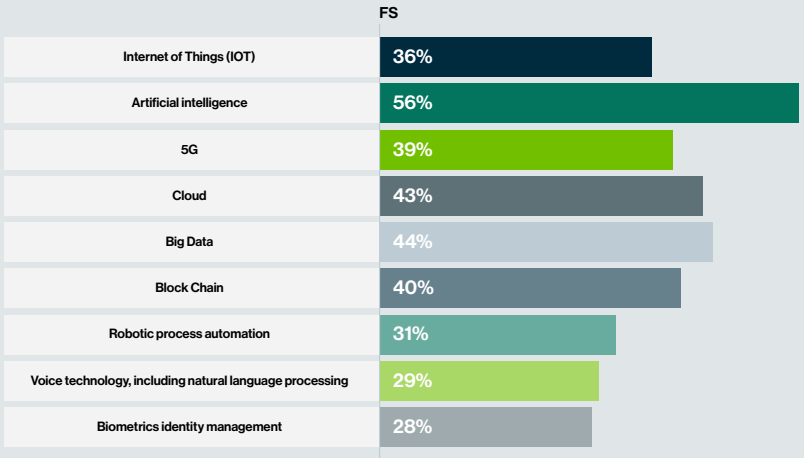
The survey also shows that the top challenge for financial services in implementing a fintech strategy are "security, compliance, and data privacy risks and related issues." Companies may not entirely understand the close relationship between these issues and the way they manage personal data — data management challenges only ranked sixth in the survey. This could be because financial services (FS) firms are using fintech in only one way — to focus on the ease of use of their digital platforms and to

provide faster services and processes. Instead, firms could also use this information to focus on improving personalization and the customer experience. Fundamentally, financial services firms need to engage with personal data successfully — which includes being compliant and ethical in the use of this data — to build and retain customer relationships.

This white paper examines some challenges that may be holding financial services firms back from engaging with personal data in a way that supports digital transformation. Next, the paper explores ways company executives could think more strategically about supporting data privacy to achieve their Data Intelligence goals. Lastly, the paper describes seven key actions to achieve Data Intelligence by implementing a holistic strategy around personal data. These are practical steps organizations can take to align investment in data privacy compliance and ethics with their digital transformation strategy.

Exhibit 1: Technologies leaders think will drive change

In your opinion, which technologies are set to transform the way financial services are delivered within the next two years?



Base: All FS respondents (248), Don't know (0%)
Source: PwC Global Fintech Survey 2019

https://www.pwc.com/gx/en/industries/financial-services/assets/pwc-global-fintech-report-2019.pdf

Grasping the challenges

Understanding that having the right data privacy approach is key to developing strong customer relationships is essential. However, being able to deliver the appropriate compliance and ethics framework, policies and processes can be a significant issue for firms today. Important challenges that financial services organizations often face include:

1. **The pace of regulatory change**
   The EU's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) are only the beginning in terms of new rules governing personal data. Within the US, this is happening on a state-by-state level at the moment, in addition to talks of a federal law. It's possible that someday there will be a global regulatory framework for data exchange, along the lines of the World Trade Organization. Today, firms face a global patchwork of rules. This can make compliance challenging if attempted on a project-per-rule basis.

2. **Unanticipated regulatory complexity**
   New data privacy laws are provoking concerns about conflicts with other regulatory obligations. For example, the requirements of anti-money laundering (AML), know your customer (KYC) screening, anti-bribery and anti-corruption programs can conflict with data privacy requirements. These financial crime rules require firms to collect, process, store and use personal data to perform a variety of tasks, including customer due diligence and transaction monitoring. Many firms are concerned that these requirements conflict with EU GDPR's "right to be forgotten." Similar conflicts can be said to exist between the EU's Markets in Financial Instruments Directive II's (MiFID II's) requirements to retain client records and GDPR's "right to be forgotten."

3. **Complexity of current data architecture**
   The majority of traditional financial firms today have deeply complex data architectures, with layers of technology systems and significant data silos. For example, sometimes mergers & acquisitions are not integrated technologically. Or firms have enhanced software by layering more code on top of the existing code base, rather than creating a new code base entirely. These, and other activities, can create a patchwork of data resources. This results in considerable operational challenges with data. For example, a consumer banking app might call on several different geographic locations for the data it uses to create a single user profile. Governing personal data use in such an ecosystem is challenging.

4. **Shift in the location of customer engagement**
   Today, customers are more likely to use a mobile banking app than visit a branch to conduct their business. Banks are under pressure to enable the entire customer lifecycle journey to happen online. As a result, banks need to ensure that their online presence nurtures the same sense of trust that bank branches used to, in the ways they handle both customer money and personal data. This challenge requires careful management of personal data through robust data privacy compliance and ethics. However, personal data also needs to be used skillfully to enhance the customer relationship while keeping their data secure.

5. **Vulnerability of third parties**
   Regulators have been highlighting the risks that third parties potentially pose to financial services firms. For example, the UK's Financial Conduct Authority (FCA) noted that IT failures at third-party suppliers are the second highest cause of disruptions to services, triggering 17% of incidents reported between October 2017 and September 2018. Although the third party may have caused the incidents, the financial services firms are the ultimate receivers of the financial and reputational changes.

The scale of the challenges above makes it clear that point solutions — which are designed only to tackle a specific data privacy issue — simply will not work.

The scale of the challenges above makes it clear that point solutions — which are designed only to tackle a specific data privacy issue — simply will not work. They are usually not enterprise-grade. Additionally, they are not capable of supporting the development of deeper and richer customer relationships, which are an essential part of digital transformation success. Financial organizations should take a more holistic approach to data privacy compliance and ethics to meet these challenges head-on.

Thinking strategically about personal data

Organizations sometimes struggle to think about the "big picture" when it comes to personal data. According to a recent survey by the Economist Intelligence Unit, 55% of respondents admitted that their overall approach to data governance was "largely driven by legal and compliance considerations." Another 44% confessed that their programs were "largely driven by privacy concerns" (e.g., marketing and/or customer concerns)." The survey also found that data governance and privacy are mostly left to the technology function, with little input from other teams. Just 40% of those who responded said their organization measured the success of its approach to data governance by looking at its contribution to strategic goals — there is not as much thinking about offensive use cases as there could be. In contrast, about half of organizations judged success by looking at the accuracy of data and compliance, a more defensive measure.

So, there is a lack of strategic thinking about the role of data, including personal data, within digital transformation. Failure to think about the bigger picture means that the five key challenges could remain unaddressed. Instead, financial services firms need to take a more offensive, strategic approach to personal data that enables them to:

1. **Overcome legacy challenges**
   Break down silos so that personal data can be found and used — compliantly and ethically — across the entire organization.

2. **Comply with agility**
   Embed a sustainable approach to regulatory change that supports a much easier adoption of future data privacy law requirements and guides the use of personal data in complex compliance circumstances.

3. **Build trust**
   The right approach to data privacy should enable firms to build trust within customer relationships. It should allow firms to be transparent about how they are compliant and ethical in their use of personal data through both words and actions. If executed correctly, the right approach to data privacy will help firms build trust with internal and external stakeholders as well.

4. **Know your customer better**
   A strategic approach to personal data should certainly enable the firm to deliver robust, trusted analytics about customer relationships to the business, senior management and the board. Best practice is to include an offensive use case of 360-degree customer analytics within personal data programs from the start.

5. **Enhance customer experiences**
   Personal data programs should also support the ability of the business to improve customer experiences. For example, data privacy frameworks should support Privacy By Design — a best practice as well as a regulatory requirement in some jurisdictions — so customers have a good experience with the firm's use of their personal data, and can act on and have control over their data privacy rights. Personalization is also an essential offensive use case that such a program should support.

6. **Connect with new partners**
   Financial firms embracing digital transformation are partnering more with other organizations for mutual strategic advantage and outsourcing to specialist services providers. Companies need to be able to manage how they share personal data with third parties, as well as how third parties share personal data with them.

7. **Innovate**
   Any data privacy program must support an organization's ability to innovate technologically. This support should go far beyond just ticking compliance boxes. The program should include elements such as data lineage, data quality and permissions so that the firm can confidently innovate while using personal data.

From this list of important needs, one can see how a project-based approach to data privacy compliance will be self-limiting for financial services firms — restricting their ability to engage in digital transformation. Instead, firms need to embrace a strategic approach that will meet these demands, enabling the firm to deepen and enrich its customer relationships through digital transformation. Financial services firms need to create a strategy that will deliver Data Intelligence.

7 actions to achieve Data Intelligence through a holistic personal data strategy

The good news is that there are seven key actions financial services firms can take on their strategic personal data journey that will lead them to Data Intelligence. Data Intelligence is the result of connecting the right data, insights and algorithms to allow all Data Citizens to optimize processes, increase efficiency and drive innovation. Data Intelligence is essential for digital transformation, and so making Data Intelligence the goal is particularly important for personal data. Personal data is vital for building deeper and richer customer relationships, but companies must handle this sensitive data compliantly and ethically. The seven key actions are:

1. **Uncover personal data throughout the organization**
   The first step toward Data Intelligence for any organization has to be to find and catalog all of the personal data dispersed across the firm. It's important to do this using a trusted, automated solution that maps relationships between data to show how personal data sets are built, aggregated, sourced and used.

2. **Create a single source of truth for personal data**
   Put all of the information about the organization's personal data in one place. Automate data governance and stewardship activities so that the management of this personal data resource scales with the growth of the business.

3. **Transform the way people think about personal data**
   Break down organizational silos alongside the technology ones. Support the cultural change that's needed to help Data Citizens communicate about and use personal data more collaboratively. Educate and enable teams to engage with training colleagues and wider communities of Data Citizens about personal data and digital transformation.

4. **Embed a sustainable approach to compliance and ethics**
   Operationalize data privacy policies and processes so that the organization's approach to compliance and ethics comes to life. Manage regulatory change by altering workflows and permissions quickly and easily. Help employees to navigate regulatory complexity through clear information about how to responsibly use personal data.

5. **Empower people to discover personal data**
   Enable business users to quickly search for and access this data for analysis and insights. As the regulatory and ethical requirements around data privacy continue to grow, it is important for organizations to enact limitations on access to and the use of personal information. Implementing a data catalog with appropriate governance processes and controls to address these challenges allows organizations to easily address these challenges.

6. **Manage personal data use with automation**
   Track how personal data is used throughout the organization, supporting compliance rules and ethics guidelines. Ensure that personal data is shared correctly with partners and third parties. Automating as much as possible of these processes reduces risk and supports innovation.

7. **Embed privacy-by-design within innovation**
   Whether firms are using personal data to improve personalization, enhance the customer experience, or develop new products and services, it's important to get data privacy right. Building in privacy-by-design is much easier when a strategic approach to personal data supports the requirements of this best practice.

These seven steps to Data Intelligence for personal data will enable a firm to address a wide range of strategic challenges. Firms can implement a sustainable approach to data privacy compliance and ethics that responds with agility to both regulatory change and complexity. Organizations can leverage this approach to achieve true Data Intelligence, delivering ways to use personal data within digital transformation projects to enhance customer relationships.

Conclusion

It's easy for financial services firms to get caught up in the teeth-gnashing and garment-shredding outbursts that fears about complying with new data privacy rules can elicit. The reality is, within a decade, such rules will be in place in nearly all jurisdictions and individuals will become more aware of the rights they have around their personal data. Firms that fail to embrace data privacy will suffer competitively.

Organizations should see data privacy compliance as an opportunity to enhance their ability to engage with personal data comprehensively — and in particular, its use within digital transformation projects. Such firms are much more likely to survive and be successful. Financial services firms that can harness their personal data to create Data Intelligence will be able to deliver digital transformation that should prove to be very competitive indeed.

For additional questions, contact us at:

United States
+1 646 893 3042

United Kingdom
+44 203 695 6965

All other locations
+32 2 894 79 60

By email
info@collibra.com