OLIVER WYMAN

POINT OF VIEW

FUTURE PROOFING PRIVACY

GDPR COMPLIANCE IN A NETWORKED BANKING SYSTEM

AUTHORS

Tom Ivell, Partner

Barrie Wilkinson, Partner

Ben Helps, CEO, Factern

MARSH GUY CARPENTER MERCER OLIVER WYMAN

MARSH & McLENNAN COMPANIES

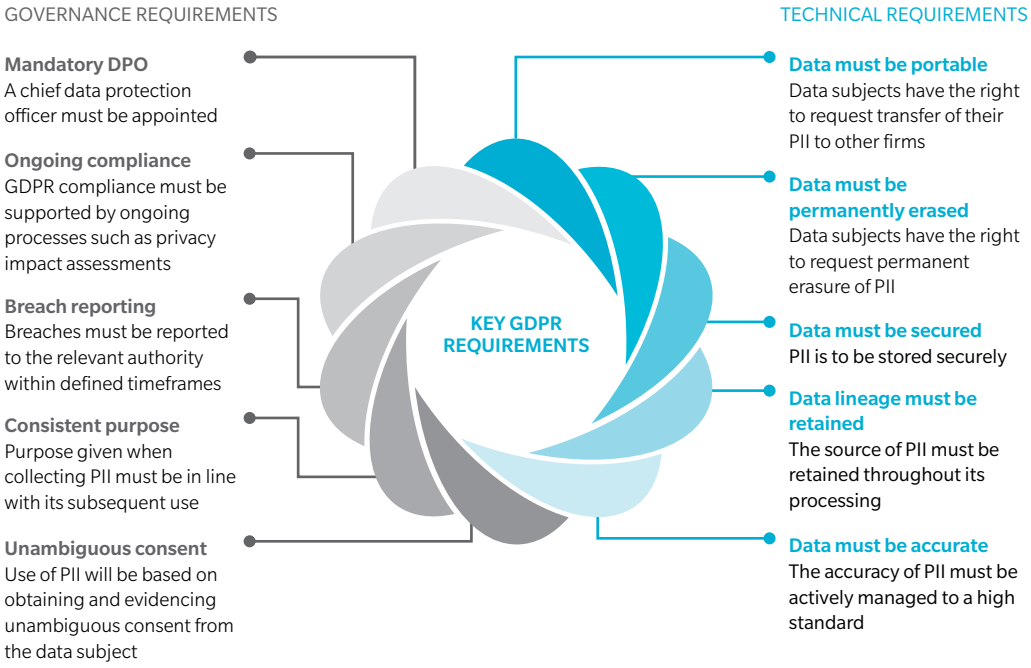
INTRODUCTION

As the volume of data being generated about individuals increases, technology is making it ever easier for that data to be transferred, and ever more powerful analysis allows valuable insights to be gained from it. How companies collect, process and protect data on their customers, staff and suppliers has turned into one of the biggest debates of our decade.

On the one hand, digitisation brings opportunity: To enhance the customer experience, to drive down costs, and to create new business models that make use of digital assets. On the other, digitisation creates a raft of new threats: whether from competitors, who use their own digital assets to disrupt existing businesses, or from cyber criminals able to steal or 'spoof' digital identities, or from fraudsters who infiltrate the digital economy to perpetrate large scale financial crime.

The General Data Protection Regulation (GDPR), due to come into effect in May 2018, is one of the European Union's (EU) legislative responses to this development. GDPR sets a common standard for how firms that operate in the EU should protect the personal data of their customers, employees and suppliers. From 2018 onwards, individuals will have a range of rights that give them greater control over their data (such as famously, the 'right to erasure') while firms will face new obligations (including capturing and recording unambiguous consent for use of personal data).

Exhibit 1: Overview of key GDPR requirements



GDPR PRESENTS A MAJOR CHALLENGE TO FINANCIAL SERVICES

The more data a firm collects, processes and shares with other data controllers, the more significant these requirements become. Financial services firms typically serve thousands if not millions of clients, deal in complex products that require access to customer data and frequent customer interaction, and often employ a large and geographically dispersed workforce.

Financial Services are also beset with a number of historical challenges, including:

- Outdated and patched-together systems resulting from several waves of consolidation, saddling firms with duplicative customer data across multiple systems
- A history of barriers to entry, prompting competition authorities to force banks to open up and provide third party service providers with access to customer data
- Years of margin pressure pushing firms towards greater use of outsourcing, with sensitive data being sent to third and fourth party providers
- Record fines and losses for anti-financial crime failings, leading to a culture of collecting as much information on customers as possible

Looking ahead, we observe a clear trend towards openness, as financial services are becoming ever more modular and therefore interconnected. New technology has made it easier for customers to buy from multiple product providers, often devised and delivered by start-up firms. Given their relative size and maturity, many such firms have incomplete infrastructure and relatively undeveloped defences against privacy breaches.

An immediate challenge is the Revised Payment Services Directive (commonly known as PSD2), which aims to create a European digital single market for payment services, and requires banks to share customer bank account data with a broad set of third party payment providers. The intersection with GDPR is clear: For the first time, sensitive, private, and personally identifiable information will be exchanged outside of the traditional payments system, requiring a fundamental rethink of the infrastructure and governance that needs to be in place.

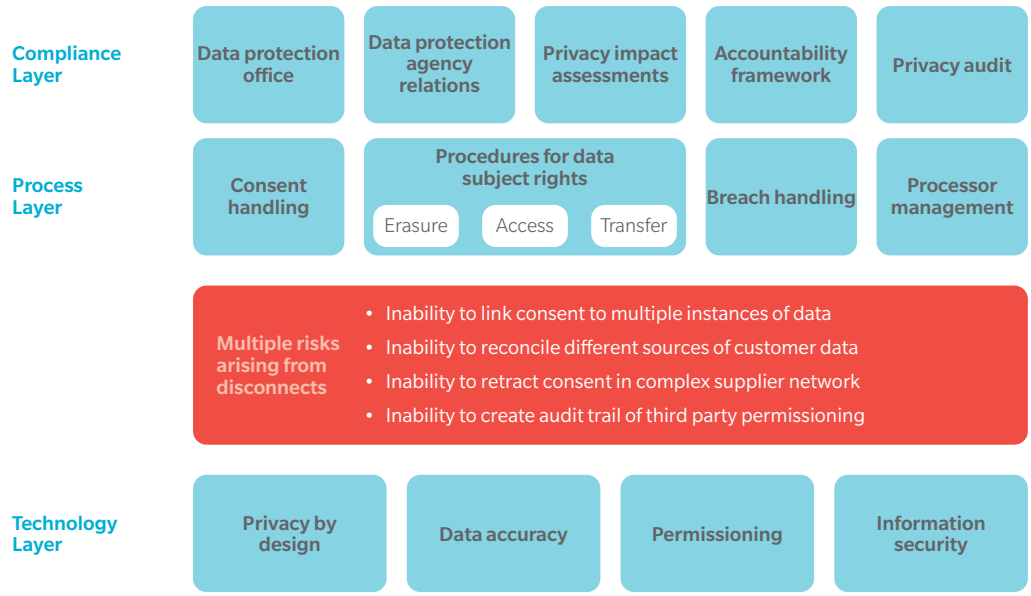
It is easy to see why financial services firms are scratching their heads on how best to comply with GDPR.

THE RISK OF AN UNSUSTAINABLE RESPONSE

At many firms, compliance programs have been devised to deliver on the formal elements required by GDPR. Policies are being drafted, data protection officers appointed, committees formed and privacy impact assessments conducted. With many programs approaching half-time, attention is turning to whether firms will make the bar the EU has set them: both narrowly for May 2018 and, importantly, on an ongoing and sustainable basis.

Many have underestimated the challenge. Those that initiated their programmes in the hope that they could meet the requirements of GDPR by focussing narrowly on the required compliance processes are recognising that the implications stretch well beyond this, involving data strategy and IT architecture, and overlapping with other regulatory changes. Historically, the biggest financial services institutions thrived as "fortresses" that securely protected the privacy of customers by trapping their data within the organisation, while offering a wide range of products to meet most needs. Today, the financial services market increasingly operates as an interconnected ecosystem of service providers, both big and small, with customer data flowing ever more freely between them. A GDPR response that does not reflect this shift through targeted changes at the technology and infrastructure layer will struggle in an interconnected future. It will at best be able to detect breaches but it will not allow active management of privacy across a firm's ecosystem.

Exhibit 2: Ignoring technology in GDPR compliance



Faced with the risk of only being able to highlight and report problems when they occur, but with few tools to make informed choices about the way that data is actually being managed, firms are now challenged to transform their privacy efforts to compete in a digital economy where huge volumes of data are being produced, combined, shared, analysed and applied (with the customer's consent) for commercial advantage.

BUILDING TRUST

In their recent publication "Welcome to the Human Era", our sister company Lippincott set out a powerful argument for the way that companies need to react to this new world. Success comes from the use of distributed rather than concentrated power structures, and

the most successful companies have recognized that "fortress" behaviour is no longer an effective approach to interacting with customers or communities.

Why? Because *"meaningful human connections can't be formed in one direction — they require the other party to reciprocate, to level with us. When they do, the connections then become a foundation for something that we intuitively understand and value highly: Trust."*

Nowhere more than in the area of data privacy is trust important. Indeed, GDPR itself is a legislative safety blanket designed to promote and enhance trust between individuals, small businesses and the institutions they deal with.

The institutions which succeed will therefore be those that do their best to uphold their side of the bargain, to be cooperative with and inclusive of their customers, employees and suppliers when it comes to handling their most private and confidential data.

Classic encryption techniques and role-based access controls – designed to prevent privacy breaches – will not be sufficient to deliver trust. Institutions need to be transparent about how they are using data, and data owners need to feel that they can influence the situation. In short, institutions need to give them back control over their own data.

PRIVACY BY DESIGN AS AN EFFICIENCY LEVER

Surprisingly to some, GDPR in fact also offers financial institutions a banner around which to rally cost saving efforts. This is because "privacy by design" requires that institutions minimise the amount of data that they collect and store in order to provide the services they offer. If executed well, this therefore generates savings.

This does not require end-to-end process redesign to ensure that no superfluous or unnecessary data is captured. Another – far more powerful – approach is for product systems to rely on data collected and stored by other product systems within the same organisation.

An equivalent comparison is the single sign on. One part of the organisation is relying on the authentication of the customer provided by another part of the organisation. The principle of reliance can be extended to attributes ("Is the customer resident in the country?", "Are they old enough to qualify for this product?") as well as data validation (e.g. confirmation of full name, contact details, etc. for the purposes of account opening).

This approach mutualises the effort involved in data processing across the organisation, not only minimising the data being held, but reducing the massive duplication of effort that routinely occurs in large, diversified firms.

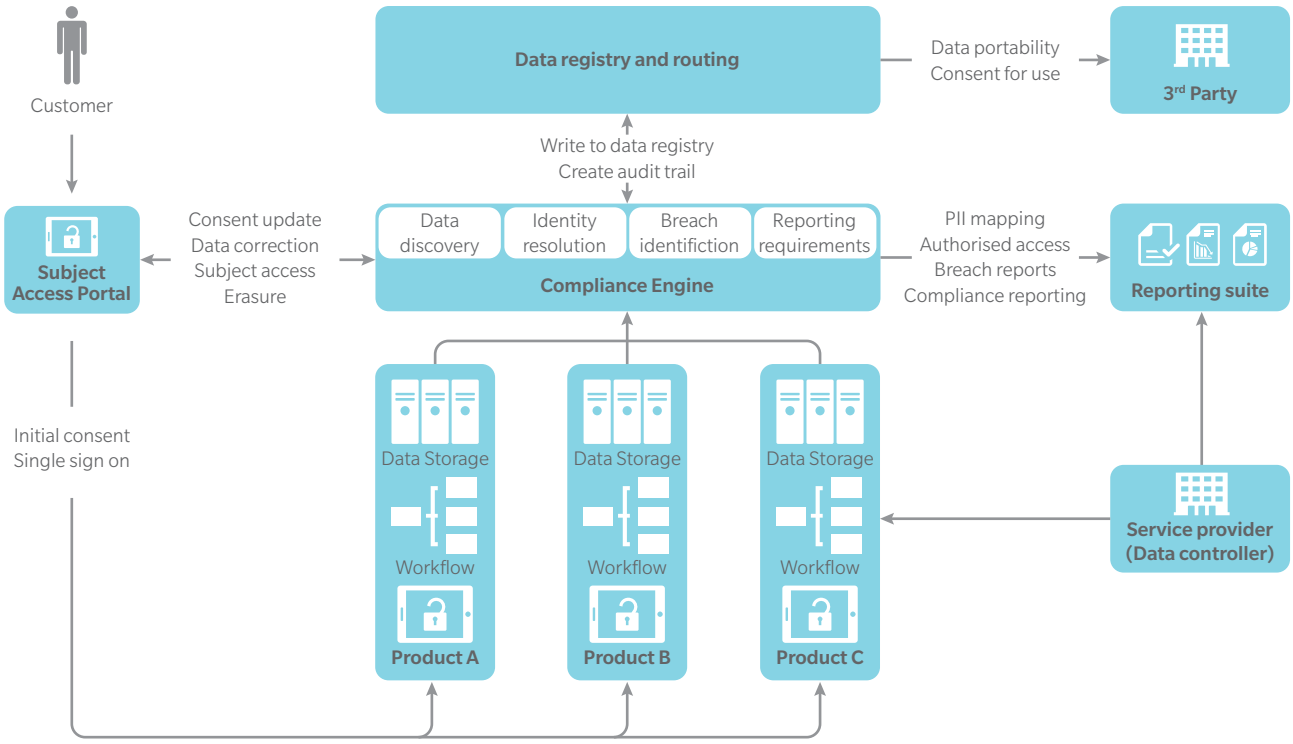
For institutions to manage "privacy by design", they must engage directly with their customers: Does the customer consent for Product B to use the data originally collected by Product A? Can the customer authenticate themselves to Product D using their log in details for Product C? This engagement is, in turn, a vehicle through which to build trust.

ELEMENTS OF A SUSTAINABLE GDPR SOLUTION

Exhibit 3 below sets out the basic components of the IT architecture that we believe will be required not only to provide a privacy solution that complies with GDPR, but also a data strategy that wins the battle for trust and facilitates a more open business model that is better suited to survive and thrive in the new digital economy.

There are already many software vendors offering compliance engines and reporting suites dedicated to GDPR. Data discovery and data mapping are often the core components of these solutions: i.e. programmes which "robotically" review existing systems, using intelligent algorithms to identify data elements that look like PII. Such programmes can help to build comprehensive views of the data network and provide logical and physical connection mapping to give a GDPR programme manager some confidence of where PII is held. They can also estimate how closely these elements are related to one another and reduce the false-positives for an auditor.

Exhibit 3: A sustainable GDPR solution in an interconnected financial ecosystem



However, data mapping tools can only ever proxy the actual provenance of data. They cannot rewind time to recreate the 'chain of custody' for each data element. For the highest priority product systems containing the most vulnerable data, it is not enough for the compliance engine to infer what may or may not be personal data on a particular individual, and to link it to another account owned by someone who may or may not be the same individual. These systems should write key meta-data directly onto a register which then becomes a factual record, or audit trail, of activity.

Firms should also be mindful of "off-line" stores of PII such as the development databases commonly used by risk analytics and model validation departments. As ever more personal and commercially sensitive data is not only produced and stored within a particular product system or firm but is also passed between those systems and firms (as a way of implementing "privacy by design" and of reducing overall operating costs, for example), then the more important it becomes that the data is permissioned, accessible, transferrable and traceable throughout an ecosystem of product systems and service providers.

A shared data register and routing system solves this problem by providing all internal product systems and – if desired – third party service providers with a single point of connectivity, as well as a 'true' record of what has happened to the data as it is either used by or disclosed between systems. The common audit trail produced becomes a key reference point for implementation of reliance schemes between counterparties, as it provides an objective, independent basis on which to assign liability in the event of a mistake or malfeasance.

The final component part of the overall IT architecture is the subject access portal. This allows customers to take full control of their own data, providing a single point through which to provide, amend and retract consent for use of private data.

Financial institutions which offer their customers a subject access portal can use it to enhance trust, by demonstrating that they take their data privacy obligations seriously and allow their customers to exercise their personal privacy rights freely.

Some financial institutions may choose to extend the scope of the subject access portal, allowing their customers to share their own data with other service providers, with the financial institution offering the latter value-adding services on top, such as identity confirmation and data validation, as a commercial activity.

PREPARING FOR THE FUTURE AND SHORT-TERM COMPLIANCE

Financial firms now face the task of reaching regulatory compliance in the short term while preparing themselves for the privacy requirements of the future. This end-state can be achieved in manageable, logical stages as outlined in Exhibit 4 below:

Exhibit 4: Five steps to sustainable GDPR compliance

- Appointment of Data Protection Officer
- Privacy impact assessments
- Assignment of accountability for data management
- Creation of program structures to implement change

- Creation of centralized data registry
- Centralization of consent handling
- Monitoring of usage against consent
- Review of subject access and breach reporting procedures

- Integration of existing systems with centralised data registry
- Redesign of customer interface to capture consent
- Creation of a factual audit trail

- Creation of customer portal to allow customer to amend the consent given, and access their own data
- Integration with third party data sources
- Integration with third party service providers

- Fostering of a market for 'input' data services (e.g. collection, storage, classification, verification, analysis) and 'output' data services (e.g. credit rating, KYC, AML, etc.)
- Outsourcing of data management to third parties

GDPR has been an important regulatory force for mobilising privacy efforts. However, it is not the end of the road. Firms looking ahead are recognising that a rethink of the underlying technology is required to remain competitive in a networked financial ecosystem. The building blocks are now available, and they can be integrated into the GDPR compliance journey without jeopardising May 2018 compliance.

Oliver Wyman is a global leader in management consulting that combines deep industry knowledge with specialized expertise in strategy, operations, risk management, and organization transformation.

Factern is dedicated to supporting data sharing in an 'open data' technology environment. Factern provides the core functionality required for data sharing; a programmable governance to ensure data is shared in a structured and secure manner, and; outreach to stimulate the creation of a networked ecosystem of the applications that benefit from an 'open data' environment.

www.oliverwyman.com

For more information please contact the marketing department by email at info-FS@oliverwyman.com or by phone at one of the following locations:

AMERICAS
+1 212 541 8100

EMEA
+44 20 7333 8333

ASIA PACIFIC
+65 6510 9700

OLIVER WYMAN