Building a better working world

GDPR: demanding new privacy rights and obligations

Perspectives for non-EU financial services firms

In the race to compete in today's digital world, organizations are using social, mobile, big data, analytics and the Internet of Things to gather as much information on their customers as possible, while simultaneously trying to do everything possible to protect their organizations from cyber risks that come from the outside and within. In this environment, privacy protection can become an afterthought, bolted on to information security programs in an ad hoc manner or, in the worst case, organizations have elected to ignore the issue.

For years, regulators and privacy commissions around the world have attempted to regulate privacy protection and develop privacy standards, such as privacy by design (PbD), for organizations to adhere and adopt. However, even as regulators pushed accountability, many organizations saw it as more voluntary than mandatory. They were content to address the letter of the law outlined in the legislation as opposed to its spirit, i.e., to meet minimal compliance obligations without taking responsibility for their role in protecting their customers' or employees' information.

With the forthcoming implementation of the European Union's (EU) General Data Protection Regulation (GDPR), and its implications for organizations across the globe, the days of organizations leaving the responsibility for privacy protection to someone else are about to end. The EU's GDPR puts the onus of specific privacy requirements in the hands of the entities collecting, storing, analyzing and managing personally identifiable information.

Firms subject to the GDPR will have to demonstrate their compliance with the requirements by May 25, 2018. The GDPR is much more demanding, and applies more broadly, than existing EU data protection requirements. Each requirement by itself – such as the right to be forgotten, data portability, 72-hour breach notification, data privacy impact assessments and privacy by design – is demanding, but in aggregate, the GDPR is very onerous.

For more cyber and privacy insights, visit ey.com/fsGDPR **or** ey.com/fscyber

Note: The General Data Protection Regulation is European Union regulation 2016/679, made 27 April 2016, implementation date 25 May 2018.

To date, many non-EU financial services firms have been slow to react to the GDPR. While some firms have taken a proactive and comprehensive approach, many have not. Even firms in the EU are delayed. For example, a recent UK government survey highlighted that only 6% of the Financial Times Stock Exchange (FTSE) 350 companies report being completely prepared to meet the GDPR compliance requirements.[1]

Firms need to focus on the GDPR now. Time is running out!

Immediate next steps

- Educate key stakeholders, including the board of directors
- Risk-assess (including legal applicability) whether the GDPR applies to your organization
- Establish cross-function and cross-business governance structure for assessment of the GDPR's applicability to business operations, evaluation of readiness and management of your overall GDPR remediation efforts
- Conduct a privacy impact assessment, with a strong focus on high-risk data flows of business processes
- Conduct a GDPR gap assessment, with a particular focus on governance, policies, technology, external dependencies (e.g., vendors), existing data flows ("high-risk") and processing operations
- Design and execute a prioritized implementation plan to address gaps based upon risk tolerance, risk priority, resourcing and investment

[1] "FTSE Cyber Governance Health Check Report 2017," HM Government, Crown copyright 2017.

What is the GDPR?

The GDPR is an omnibus data protection law that builds upon, expands and ultimately replaces the EU Data Protection Directive. The GDPR gives individuals new rights over their data, which heightens the accountability on entities collecting, storing, analyzing and managing personally identifiable information. This covers any information relating to an identified or identifiable natural person, such as name, identification number, location data or one of more factors specific to physical, physiological, genetic, mental, economic, cultural or social identity on the nature of the person, as well as online identifiers (e.g., IP addresses). A data subject can be a customer, employee, contractor or third party. Released in 2016, and due to come into effect May 25, 2018, the GDPR applies to any organization, regardless of geographic location, that controls or processes the data of an EU resident in a proscribed way. It dictates to what extent personal data may be collected, the need for explicit consent to gather such data, requirements to disclose breaches of data and stronger powers to substantially fine organizations that fail to protect the data for which they are responsible. And it has real teeth.

The GDPR prescribes certain responsibilities and liabilities to controllers and processors of personal data. It is important to understand these terms as they are defined within the GDPR.

- **Controller:** a body (alone or jointly with others) that determines the purposes and means of the processing of personal data
- **Processor:** a body that processes personal data on behalf of the controller; processing activity can include collecting, organizing, storing, disclosing, using, etc.
- **Personal data:** any information (single or multiple data points) relating to an identified or identifiable natural person such as name, employee identification number or location data

The GDPR imposes new obligations on both controllers and processors of personal data, emphasizing accountability and requiring greater documentation and records.

Firms have until May 25, 2018, to implement changes and comply with the obligations of the GDPR. Penalties for failing to comply with the GDPR's basic processing principles may subject the organization to fines up to €20 million or 4% of the organization's total global revenue, whichever is greater.[2]

Key facts about the GDPR

Applicability: applies to entities – including third parties that are (i) established in the EU, (ii) providing goods or services to EU residents or (iii) are monitoring the behavior of individuals in the EU

Fines: up to €20 million or 4% of the organization's total global revenue, whichever is greater; also provides individuals new rights to bring class actions against data controllers or processors, if represented by not-for-profit organizations, which heightens litigation risk

[2] EU regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

GDPR highlights

Organizations will have only 72 hours to report data breaches.

Privacy-by-design principles must be incorporated into the development of new processes and technologies.

Explicit and affirmative consent will be required before processing personal data.

Most organizations will need to designate a Data Protection Officer.

Organizations will have to maintain records of processing activities.

Organizations will need to scale security measures based on privacy risks.

International transfers are prohibited except through certain mechanisms.

Organizations will report to one supervisory authority.

Organizations will have to facilitate customers' and employees' right to erasure (of data), right to portability, and an increased right of access.

GDPR impacts

Penalties for failing to comply with the basic processing principles of GDPR may subject the organization to fines up to

€20 million or **4%**

of the organization's total global revenue, whichever is greater.

Organizations have only until

25 May 2018

to implement changes and comply with GDPR obligations.

Imposes new

obligations

for both controllers and processors of personal data

Places a greater emphasis on

accountability

requiring greater

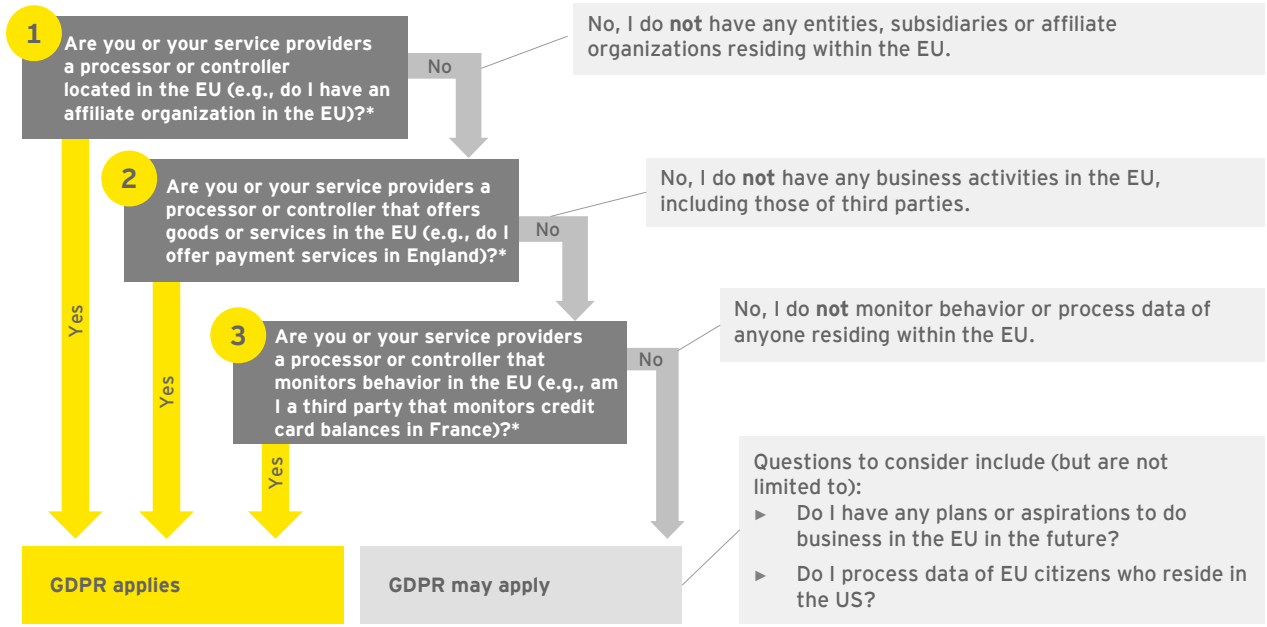
documentation

and records

Is the GDPR applicable to you?

Many non-EU financial services firms have determined that the GDPR doesn't apply to them with limited understanding of how the regulation actually works. Figure 1 outlines three distinct questions that can be used to assess applicability.

Figure 1: Three key questions to assessment applicability



***Note** – the responses to these questions should be evaluated based on the facts and circumstances in your organization and discussed with legal counsel.

The question, "Are you or your service providers a processor or controller that monitors behavior in the EU?" captures a broader range of activities than many firms think. Consider centralized functions that conduct surveillance, such as for fraud, anti-money laundering, sanctions or cyber threats. To the extent those functions use data related to EU residents, your organization may be subject to the GDPR requirements. Similarly, many firms' websites continuously monitor traffic and users, and some leverage third-party vendors in the website execution. Those activities – of the firm or the third parties – may subject your organization to GDPR requirements.

Firms are advised to consider these questions and discuss them with their legal counsel. However, firms may be inclined to take too much of a legalistic approach to the GDPR, depending too heavily on outside counsel's advice on whether or how the GDPR applies to their firm. In addition to the legal input, firms should undertake a risk-based assessment to evaluate the relevance and applicability of the GDPR based on a fact-based, documented review of the degree to which their operations or third parties access, store or monitor data related to EU residents. Such an approach takes into the account the firm's strategy, growth plans, risk tolerance, existing controls and capabilities, as well as other contextual factors that may impact the determination of applicability.

What are the main GDPR concepts and requirements?

The GDPR enhances the data protection rights of EU data subjects. In general, firms will need to provide easier access to personal data, with clear and understandable information on its processing, use and storage.

Major requirements and concepts include:

- **Data protection impact assessment (DPIA):** DPIAs (also known as a privacy impact assessment or PIA) are required for all process operations of an organization. DPIAs should be viewed as tools that can help organizations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. There is a debate in the marketplace about the required approach: are data flows required for GDPR or can data narratives be utilized? Generally, firms seem to be completing data flows to properly assess the GDPR, especially to understand data flows in their high-risk processing activities. An effective DPIA will allow organizations to identify and fix problems, reducing the associated costs and damage to reputation that might otherwise occur.
- **Data privacy accountabilities:** the GDPR attempts to define what privacy accountability means in practice through requirements around proactive monitoring and personal data records. The GDPR states that the controller is responsible for confirming that all of the GDPR privacy principles are adhered to and that firms can demonstrate compliance. Each organization has to understand the principles of lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation and integrity and confidentiality. The DPIAs will help in this regard.
- **Condition for processing:** the processing of personal data is only lawful if it is permitted by the GDPR and has proper customer consent. If the controller does not have a legitimate reason for a given data processing activity, then that activity is not allowed – firms must have at least one legitimate reason for processing, which can include the individual's consent, contractual necessity, legal obligation, regulatory requirements or public interests.
- **Data protection officer (DPO):** firms that establish they conduct large-scale systematic monitoring of EU residents' data or process large amounts of sensitive personal information have to appoint a DPO. "Large-scale" could be as small as the processing of data on more than 5,000 subjects in any 12-month period.[3] DPOs have significant accountability for adherence to the GDPR requirements, and they must be appropriately qualified in data protection laws and practices, independent of management,have access to the necessary resources to monitor GDPR compliance and be actively included on all relevant data protection discussions and decisions. The regulation calls for the DPO to report to the "highest management level," which EU guidance suggests could be the board of directors.[4]
- **Privacy by design (PbD):** is the practice of establishing and implementing privacy controls and principles into business processes and systems as they are being developed and built, rather than layering on controls after deployment. Although PbD has been championed for years by privacy commissions around the world as a leading privacy standard, in our 2015 Global Information Security Survey, only 18% of survey respondents indicate that they have applied PbD to their new processes and technologies.[5] Under the GDPR, organizations will now be required to design policies, procedures and systems that follow PbD principles at the outset of every product or process development.
- **Right to erasure:** the right to erasure enables an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing. This right creates significant data retention challenges for firms. The broader EU principle this relates to is the right to be forgotten, whereby residents have the right to have personal data on public media deleted (including by third parties).

[3] "Top 5 Priorities to Prepare for EU GDPR," *Gartner website*, www.gartner.com/smarterwithgartner/top-five-priorities-to-prepare-for-eu-gdpr, 20 June 2017.

[4] Article 29 Data Protection Working Party, Guidance on Data Protection Officers (DPOs), April 5, 2017.

[5] *Can privacy really be protected anymore? Privacy trends 2016,* EYGM Limited, 2016.

- **Individuals have the right to have personal data erased and to prevent further processing:** under the following circumstances:
  - Personal data is no longer necessary in relation to the purpose for which it was originally collected/ processed.
  - Individual withdraws consent.
  - Individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
  - Personal data was unlawfully processed.
  - Personal data has to be erased in order to comply with a legal obligation.
  - Personal data is processed in relation to the offer of services to a child.
- **Consent and notifications:** under the GDPR, consent must be freely given, specific, informed and unambiguous, indicating the data subject's agreement to the processing of personal data relating to him or her. It should be noted that consent is not required if there is another basis for use — in practice, most firms will point to a signed contract as their basis.

  Breach notifications under the GDPR must be done within 72 hours of the organization becoming aware of the breach. If the breach is sufficiently serious to warrant notification to the individual data subject, the organization responsible must do so without undue delay. Failing to notify or noncompliance can result in a significant fine up to €10 million or 2% of global revenue.[6] Many practitioners expect that when the EU issues new guidance later in 2017 on the breach requirements, it will recognize that it will often be impossible to investigate a breach fully within that time period and will allow firms to provide information in phases, so long as the relevant data protection authority, or DPA, is notified.
- **Data portability:** the right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. The provision allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. It is the responsibility of the controller to confirm this capability exists.

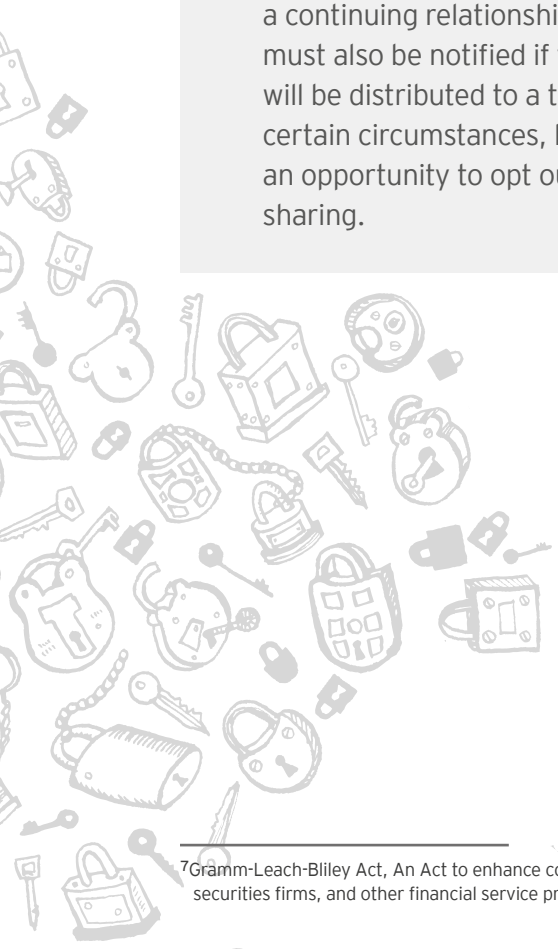
[6] EU regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

What is the difference between EU GDPR and US GLBA?

The focus of all privacy regulations is on an individual's right to control access to the personal information that is collected, used (processed) and shared. However, while sharing a common goal of protecting an individual's personal information, the GDPR and US-based Gramm-Leach-Bliley Act[7] (GLBA) differ in approach.

- GLBA, enacted in the US in 1999, indicates that privacy requirements are dependent upon the extent of a financial institution's **continuing relationship with the "consumer"** (i.e., a one-time transaction between financial institution and the consumer would not apply as a continuing relationship). Consumers must also be notified if their information will be distributed to a third party, and in certain circumstances, be presented with an opportunity to opt out of information sharing.
- The GDPR expands what constitutes personal data and mandates that **all institutions maintain the EU resident's right to privacy irrespective of the current relationship** (i.e., heightened security standards apply even after the EU resident cancels their accounts).

These fundamental differences in approach, along with the specific technical requirements outlined in the GDPR, mean that organizations cannot rely on GLBA compliance as an indicator of GDPR compliance. Indeed, firms have to appreciate that GLBA relates mainly to the *sharing* of information, whereas the GDPR relates to the *processing* (collection, use, storage, sharing, retention, etc.) of information. As such, a separate and thorough GDPR assessment is necessary.



[7] Gramm-Leach-Bliley Act, An Act to enhance competition in the financial services industry by providing a prudential framework for the affiliation of banks, securities firms, and other financial service providers, and for other purposes, enacted by 106th United States Congress, effective 12 November 1999.

What are some common misconceptions around the GDPR?

There has been a relatively slow response by many non-EU financial services firms to addressing the GDPR. It is difficult to determine what accounts for this general lack of action. It could be that some firms have, incorrectly, viewed the GDPR to be a continuation of existing EU data protection requirements, so no real change is required. Some firms may have seen a May 2018 implementation date and determined there is ample time to act. Some firms — perhaps many — may feel the rule doesn't apply to them, given it's an EU regulation. Some may have assumed their European teams have this in hand — after all, it's an EU regulation

Whatever the reason, more non-EU firms are now starting to realize that the GDPR may apply to them, and when it does, that it is very demanding. As they do, they should be careful about making some common mistakes:

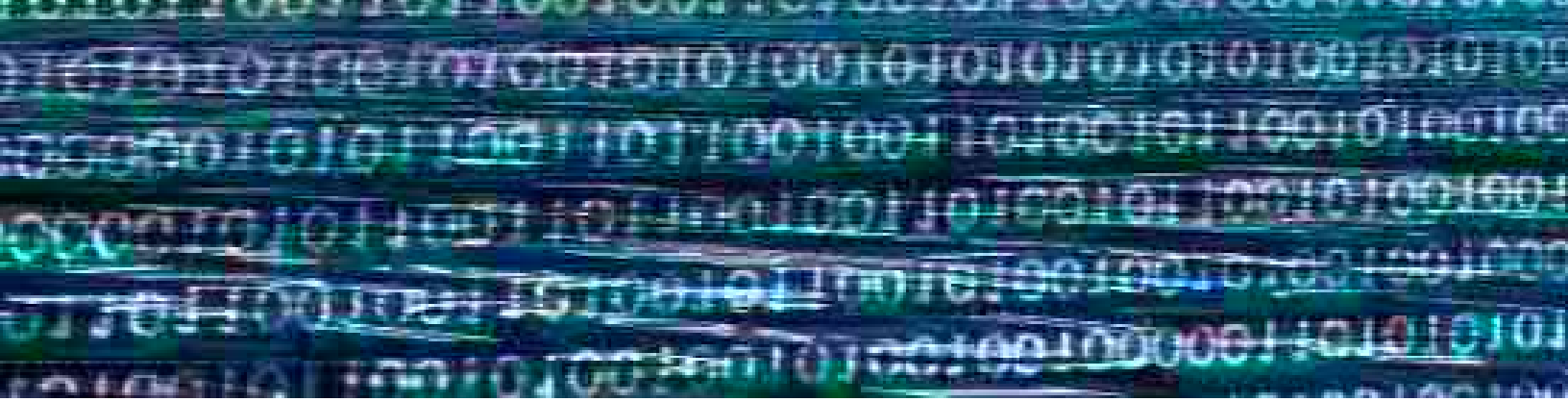
- **Underestimating the level of effort:** often as a result of misunderstanding the breadth, potency and applicability of the GDPR, firms have underestimated the level of effort required to evaluate the applicability of the GDPR, and where it applies, to implement the necessary changes to become compliant. The reality is that the GDPR affects a broad swath of the firm and requires action by a large set of professionals in the businesses and many functional areas (see below). For non-EU firms, it requires a significant degree of cooperation and collaboration between the home office and operations in Europe, as well as with relevant third parties.
- **Underestimating the breadth of impact:** the GDPR may require significant changes to the way firms operate, including their data management strategy, management of customer consents, management and oversight of third parties, the approach to product development, marketing, applications, notifications and other disclosures, potentially firms' business models, the transportation of data across borders, outsourcing contracts and much more. These impacts are likely material and will take time to fully identify, consider and address.
- **Thinking it's easy to identify EU residents:** in practice, it is hard for firms to identify who within their customer base is an EU resident. To the extent that firms have gathered full residentship data, it is easier. Identifying European mailing addresses as primary residences will also help (including non-EU residents living in the EU, as it applies to them, too). Identifying the number of EU residents within the customer base will be a major determinant of the extent to which the GDPR applies and how much of its impact can be quarantined to specific business, geographies and data sets.
- **Viewing the GDPR as only relevant to retail businesses:** given that the requirements center on EU residents' data, some firms may think incorrectly that it only relates to retail businesses. However, some corporate clients — for example, small and medium-sized businesses — often use personally identifiable information, such as personal addresses and tax or national security numbers, as part of their customer data or during the client acceptance process. To the extent they do, that could mean the GDPR applies to businesses serving those clients, as well, depending on whether the firm trips GDPR compliance, as noted above.
- **Viewing it as a one-and-done exercise:** perhaps the most significant challenge is redesigning a firm's privacy and business processes to be able to demonstrate GDPR compliance on an ongoing basis, especially as the business, client base and product portfolio evolve, and to periodically reassess whether GDRP applies to the firm. Getting to a position of GDPR-compliance is the end of the beginning. Compliance is an ongoing responsibility and, if anything, it will be the inability to execute on GDPR commitments (e.g., enabling customer data portability or maintaining customer consents to use the data as required) on an ongoing basis that will put a firm at the most risk of regulatory penalties and/or customer class action suits. Building in sustainable approaches that provide the firm with the necessary flexibility to redesign how it develops and delivers products and services to its customers is most critical.

Which parts of your organization will be most affected?

The GDPR will have a significant impact across a firm's three lines of defense:

First line (business lines and technology)

- **Business lines:** like other risks, the front-line businesses have to own the risks they create, including privacy and data protection. They have to identify, measure, monitor and mitigate the risks associated with the GDPR, implement the privacy principles, and design and maintain necessary and effective controls. They also have to implement enterprise-wide risk management frameworks developed by the second line, including in this context privacy risk, information technology risk, operational risk and overall enterprise risk management.
- **Operations:** those running day-to-day operations have to develop and implement the necessary standards and procedures that secure personal data through the data life cycle and conduct DPIAs to properly understand and manage the inherent risks. They also tend to be the vendor relationship owners, so they have to manage relevant third parties so that they remain in line with the firm's privacy and GDPR requirements and obligations.
- **Technology, security and data:** the technology group will have to consider what changes are required to the technology and data architecture to enable the proper handling, processing and security of relevant customer and employee data. This will include how the data is gathered (and through what channel), processed, stored, transferred (including cross-border and to other firms) and, when necessary, destroyed. Tracking what data is affected will be a significant effort, especially as it relates to customer and account book-of-record, employee or contractor data (e.g., time and reporting systems)[5], personal data used in customer relationship and marketing databases, and so on. The data management strategy that firms may need to adopt to effectively execute against GDPR requirements — in terms of tagging (including geotagging), tracking, anonymizing, encrypting, quarantining and making destroyable (in actuality or in effect) — could be onerous, depending on how the firm determines it will address GDPR compliance. Those driving data analytics activities have consider how they may be affected.
- **Customer relationship management (CRM):** firms will need to re-evaluate their CRM strategy and data management to determine if more client segmentation is required, from a perspective of quarantining EU residents' data and in terms of how customer data is used to target products and services.
- **Innovation and marketing:** product development activities may need to be evaluated to determine how GDPR considerations are built into the new products and services, as well as how customer-facing design activities — such as customer surveys and focus groups — may need to be adapted. Marketing materials will need to be revised to include the necessary disclosures, consents and notifications. Consent is one of the largest areas of challenge, especially around the need to consider whether you can 'grandfather' existing consent or whether you need to run a 'retrospective re-consent' exercise.
- **Procurement and contract management:** procurement and legal teams may need to evaluate existing standard contractual template terms to understand whether amendments are required to meet the GDPR requirements – for example around the 72-hour breach notification and increased obligations on data processors. Organizations will need to identify which vendors are processing personal data and a perform a risk-based prioritization exercise to review existing contracts, identify required legal term changes, and potentially re-negotiate and 're-paper' existing contractual arrangements.
- **Human resources (HR), training and communication:** HR will need to consider if changes are required in regard to how employee or contractor data is segmented and managed, how HR data is reported upon and appropriate



employee rights and consents are managed and adhered to. Working with the relevant functions and businesses, HR will need to re-evaluate the portfolio of awareness-raising, training and education activities and how those activities remain current and effective.

First/second line of defense

- **Third party risk management (TPRM):** given the way in which the GDPR applies to third parties, the second-line TPRM group will need to re-evaluate their third party risk management framework and how the first line is adapting their standards and procedures to align with the GDPR.
- **Surveillance and monitoring:** as noted above, to the extent firms have centralized some of their surveillance activities and in so doing are monitoring activity and behaviors of EU residents, those functions may create GDPR obligations that apply to some or all of the data, depending on how it is processed and stored. The same is true of website traffic and user monitoring activities. Assessing if and how EU resident data is used in these activities will be important to determine applicability, but may also drive firms to segment those activities more than at present to isolate the degree to which those functions are impacted by the GDPR.

  Consideration should be given to the monitoring activities conducted by the second (and sometimes first) line, including anti-money laundering, sanction and fraud surveillance — or broader testing activities — so that those activities are GDPR-compliant, where relevant.

Second line of defense

- **Compliance, privacy and security:** the DPO has a critical role in this regard, working with other functional teams. The compliance function will have to validate that the privacy and data security strategy aligns with legal requirements, annual regulatory reporting requirements and broader compliance reporting and surveillance strategies. Compliance will need to develop a robust monitoring and testing program for GDPR, which can be leveraged by the DPO, among others.

  The privacy groups will need to review and revise data policies, as well as confirm that front-line standards and procedures are in line with those revisions and assess they are implemented effectively (either through reviewing first-line testing or conducting its own). Privacy notices will need updating, along with exemptions, exclusions and disclaimers and personal data definitions. Data breach processes will need evaluating so that the firm can meet its GDPR 72-hour notification requirements, including where breaches occur within third parties. The privacy group will need to confirm that data subject rights and data security standards are adhered to, in light of more demanding GDPR requirements. Privacy and data governance structures and roles and responsibilities will need re-evaluating, including the assignment of data protection officers and their working relationship with chief privacy officers.
- **Risk management:** ultimately, second-line risk, working with the compliance and privacy functions, needs to measure and monitor overall privacy and information-security — working with the DPO, who is directly responsible for monitoring — and set tolerances for such risks within a firm's risk appetite framework. This is particularly important for the GDPR given the potential for material fines and class action legal settlements. Firms will need to re-evaluate privacy-risk reporting in this context.

Third line: internal audit

Internal audit will need to adopt its approach to consider the GDPR within a number of audits, notably:

- Compliance monitoring programs
- Reviews of access processes and procedures
- Overall privacy framework validation

In re-evaluating its coverage model, internal auditors should monitor a distinct set of privacy and compliance key performance indicators, as well as potentially some that are specific to the GDPR. Some firms' internal audit groups may perform pre-implementation advisory audits, given the breadth of the requirements and the potential size of fines and settlements, or build assessments on the implementation of privacy by design principles into other relevant audits they perform.

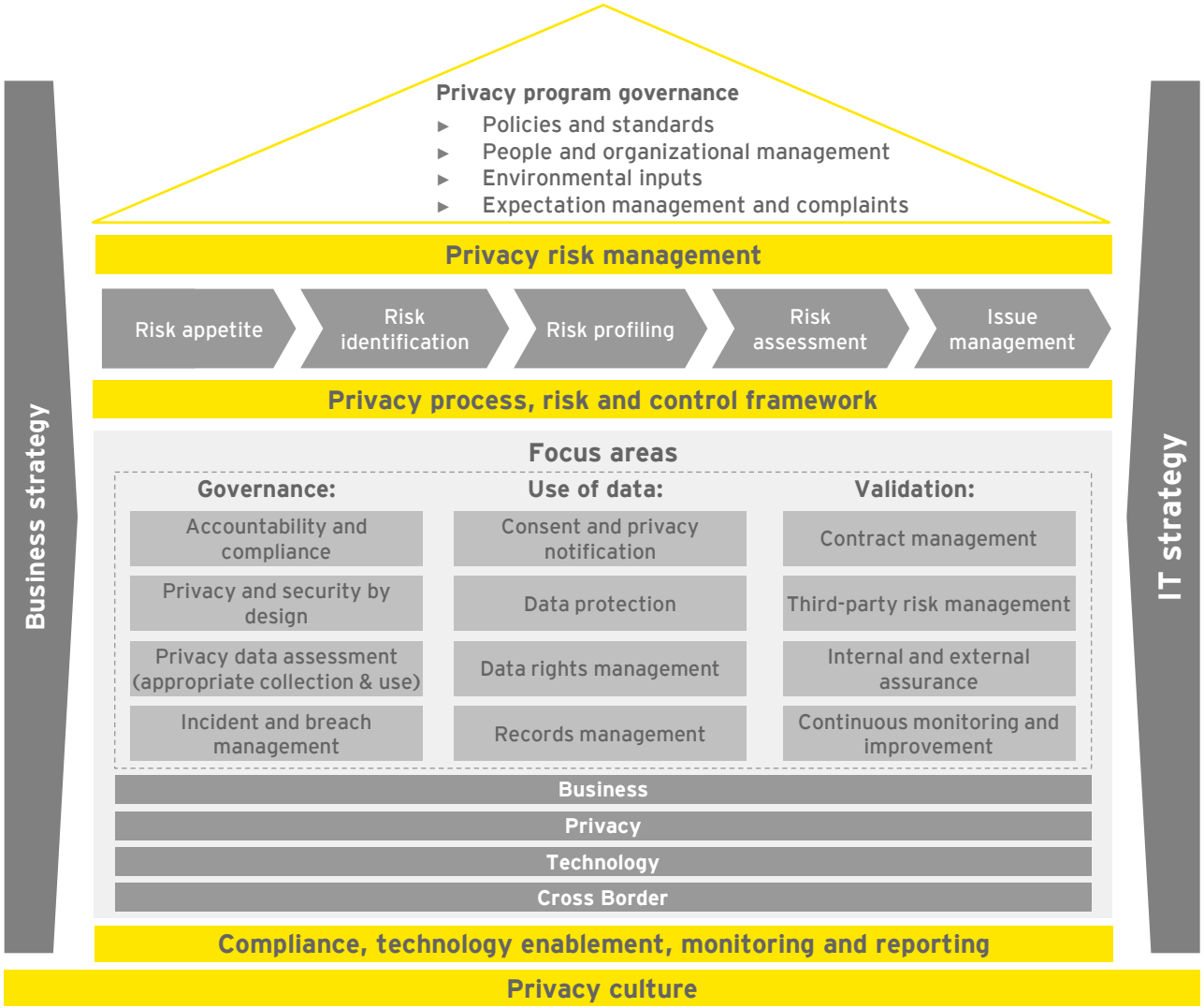
How should you implement the GDPR?

Implementing the GDPR should be viewed as an integrated exercise set within each firm's overall privacy risk management framework. GDPR touches on all aspects of an organization, reaching across people, processes and technology and, as such, establishes a cross-functional team that supports the transformation of the company, which is a critical step for a successful implementation.

EY has developed our own proprietary framework (see figure 2),which links risk management, compliance, privacy and governance with key privacy domains and allows our teams to put privacy in the context of each firm's business and information technology strategy. The framework allows firms to set the privacy strategy within the context of the firm's overall business and IT strategy, and focus on:

- **Program effectiveness:** there has to be an enterprise view of the firm's privacy program, which allows for firm-wide oversight of the program, program-level reporting and escalation, and the application of consistent policy and standards.
- **Privacy risk management:** privacy risk needs to be well managed, in a way that is consistent with the firm's overall risk management strategy, covering the risk life cycle, from risk appetite to risk identification to risk assessment to issues management. The overall privacy framework should link to the firm-wide process and risk and control framework, as well as the third-party risk management program. The various roles and responsibilities across the different lines of defense and functions (compliance, legal, privacy, cyber, etc.) should be clearly defined.
- **Compliance and monitoring:** compliance with relevant rules and regulations should be hardwired into the framework, with robust, ongoing program, compliance and privacy risk reporting to senior management and the board.
- **Data and breach management:** the firm's privacy risk strategy has to be firmly linked to the strategy for managing data, including collecting, processing, storing and destroying data. The data architecture, classification and flows have to enable the firm to conform with its privacy strategy, meet compliance requirements and support customer rights, and meet ever-more challenging incident breach and notification requirements.
- **People and culture:** the talent requirements to properly implement the privacy framework need to be spelled out, and plans need to be in place to confirm the needs are met. This includes the front-line-business talent requirements. After all, those on the front line manage privacy risk on a day-to-day basis. Privacy also needs to be firmly embedded in the firm's culture, with active, ongoing awareness programs and training.

Figure 2: EY's privacy risk management framework



To support business stakeholder understanding of privacy, and the impact of the GDPR on business lines and functions, EY applied its privacy framework to the GDPR and categorized 12 focus areas into 3 themes, as shown in Table 1.

Table 1: GDPR requirements across the EY privacy risk management framework

	Focus area	Desired outcome
Governance	**Accountability and compliance:** privacy operating model, training/awareness, policy development	Creating structures and processes that enable proactive, systematic and ongoing compliance reporting for senior management
	Privacy and security by design: privacy impact assessment, program design based on business model	Achieving risk reduction and management through the application of requirements and tools integrated at various junctures in your process landscape
	Incident and breach management: data incident response plan, 72-hour operational effectiveness process	Enabling rapid management of a data breach, including internal investigations and external reporting
	Privacy data assessment: data use case management/framework, data classification, data flow mapping, data discovery, cloud discovery, high-value asset identification	Establishing and operationalizing governance over personal data usage and analytics as well as understanding the most meaningful attributes of your data that impact compliance risk and optimized use
Use of data	**Consent and privacy notification:** freely given and explicit consent, right to withdraw consent, privacy notices	Increasing transparency through explicit consent to process data and privacy notifications
	Data protection: identify and access management, technology selection, encryption strategy	Approach designed to achieve data protection and enhance your security hygiene
	Data rights management: data subject's right to access, correction, erasure, portability and/or objection	Empowering your organization to support data rights to access, deletion, portability and rectification
	Records management: attach requirements to physical files, electronic documents and emails	Strategy and program design that balances global privacy regulation with data protection, legal and business needs
Validation	**Contract management:** assessment of service-level agreements, assess internal or third-party contracts to identify gaps or identify opportunities to strengthen language	Discovery and revision of contractual provisions pertaining to privacy and security, including data permissions and restrictions
	Third-party risk management: third-party risk assessment, compliance monitoring and data controls	Understanding, designing and monitoring for the management of your third-party personal data access, protection, responsibilities and liabilities
	Internal and external assurance: internal audit assessment, third-party attestation, certification against industry standard	Providing independent confirmation that governance, risk management and internal controls as they relate to both privacy and security are designed and operating effectively
	Continuous monitoring and improvement: compliance monitoring program design, monitoring of key controls, dashboard reporting for management	Designing for ongoing awareness of privacy and security compliance to facilitate risk management and optimization of the control environment

The clock is ticking: act quickly

In enacting the GDPR, the EU gave companies two years to get ready to comply. When enacted, this was viewed as providing sufficient time.

Now, with limited time remaining, many non-EU financial services firms still have a long way to go to validate if the regulation applies to them and, if so, to make all of the necessary changes to be ready for the May 25, 2018, implementation date. Building an approach that is sustainable beyond that date is even more challenging.

Time is of the essence. Non-EU financial services firms need to act quickly.

The first step is assessing applicability; here, a risk-based (not just legalistic) assessment is strongly suggested.

For firms impacted by the GDPR, it is important that the right governance and program structure is put in place from the outset. A cross-functional, cross-business team is required. To be successful and sustainable, this effort cannot be buried in legal and compliance.

A thorough GDPR gap assessment is needed, one that reaches across the swath of affected businesses and functions. To the extent that the assessment is too narrow, it will make timely implementation much harder. Important factors will be identified too late, causing decisions made to degrade the quality of the approach, leave the firm open to regulatory scrutiny and ultimately cost more as work needs to be redone to make the approach sustainable on an ongoing basis.

And, finally, there is a need to prioritize. After all, the timeline to implementation is getting shorter, so firms need to prioritize those activities that get to baseline compliance. Building more sustainable processes can be completed after May 25, as necessary.

It is time to act.

EY contacts

Americas

Cindy Doe
+1 617 375 4558
cynthia.doe@ey.com

John Doherty
+1 212 773 2734
john.doherty@ey.com

Ed Keck
+1 216 583 1296
ed.keck@ey.com

Angela Saverice-Rohan
+1 213 977 3153
angela.savericerohan@ey.com

Mark Watson
+1 617 305 2217
mark.watson@ey.com

EMEIA

Tony de Bos
+31 88 40 72079
tony.de.bos@nl.ey.com

Steve Holt
+44 20 7951 7874
sholt2@uk.ey.com

Asia-Pacific

Jeremy Pizzala
+852 9666 3428
jeremy.pizzala@hk.ey.com

For more cyber and privacy insights, visit ey.com/fsGDPR **or** ey.com/fscyber

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

EY is a leader in serving the global financial services marketplace
Nearly 51,000 EY financial services professionals around the world provide integrated assurance, tax, transaction and advisory services to our asset management, banking, capital markets and insurance clients. In the Americas, EY is the only public accounting organization with a separate business unit dedicated to the financial services marketplace. Created in 2000, the Americas Financial Services Organization today includes more than 11,000 professionals at member firms in over 50 locations throughout the US, the Caribbean and Latin America.

EY professionals in our financial services practices worldwide align with key global industry groups, including EY's Global Wealth & Asset Management Center, Global Banking & Capital Markets Center, Global Insurance Center and Global Private Equity Center, which act as hubs for sharing industry-focused knowledge on current and emerging trends and regulations in order to help our clients address key issues. Our practitioners span many disciplines and provide a well-rounded understanding of business issues and challenges, as well as integrated services to our clients.

With a global presence and industry-focused advice, EY's financial services professionals provide high-quality assurance, tax, transaction and advisory services, including operations, process improvement, risk and technology, to financial services companies worldwide.

EYG no. 05767-171Gbl
1709-2407447 BDFSO
ED None

ey.com