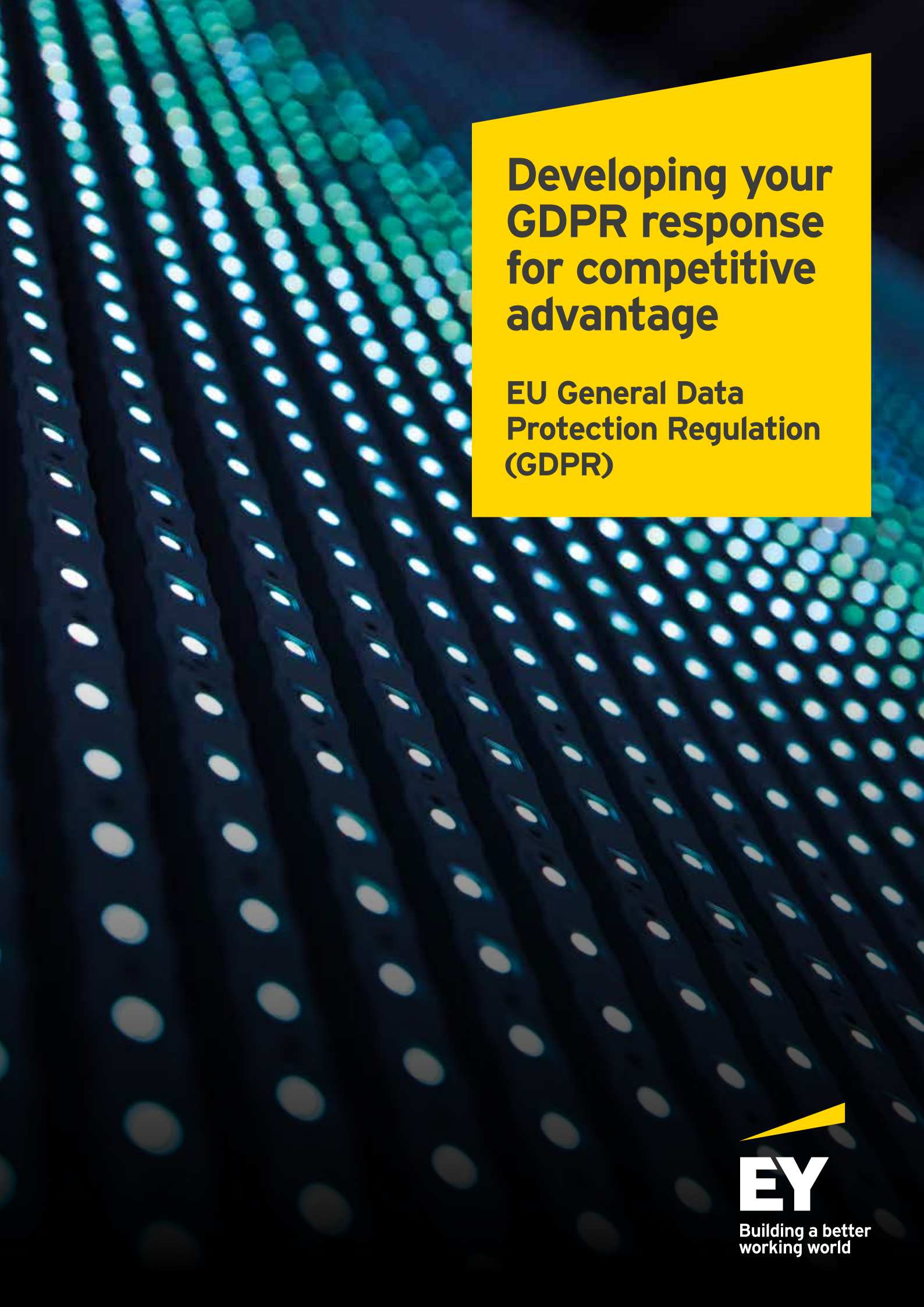


Developing your GDPR response for competitive advantage

EU General Data Protection Regulation (GDPR)

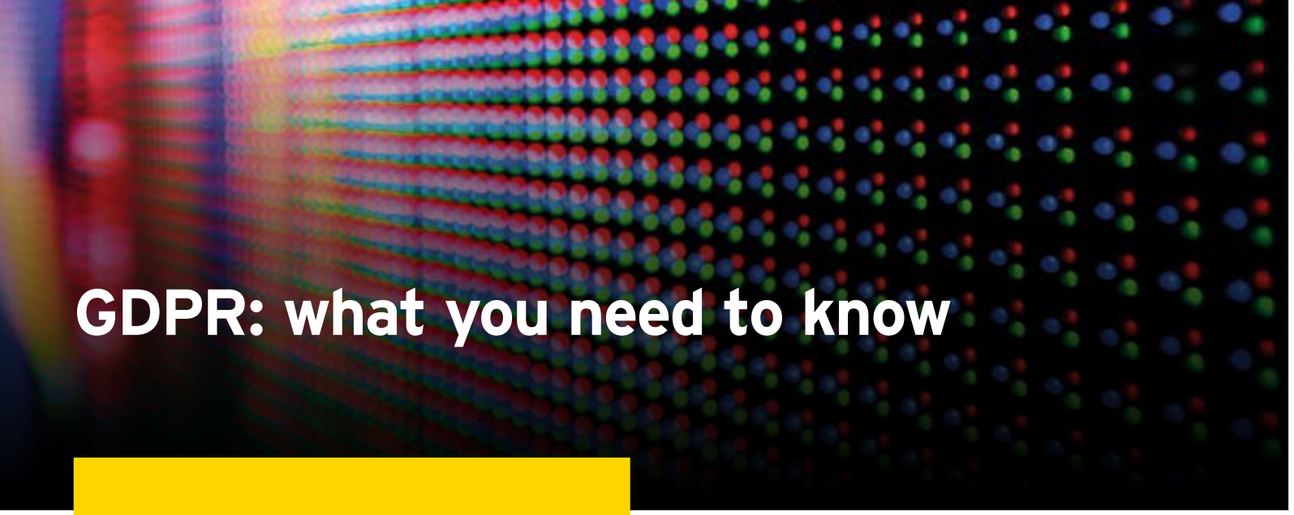
EY
Building a better working world

Introduction

In May 2018, the EU's new GDPR ushers in unprecedented levels of data protection for EU residents, backed by fines of up to **€20 million or 4% of global revenue, whichever is higher.**

A global game changer, no organization storing or processing the personal data of EU residents can afford to be complacent, wherever the organization is based and irrespective of its current privacy maturity level.

As well as the urgency of working towards compliance there is also the opportunity to take a strategic approach to GDPR. EY's risk-based, multi-disciplinary approach targets GDPR investment where it matters most for regulatory compliance and competitive advantage. Drawing on our extensive privacy knowledge and proven tools and methodologies, we help to identify clients' highest risks, and design and execute a tailored road map for compliance and beyond.



GDPR: what you need to know

When GDPR comes into force, it will introduce a raft of new rights for individuals and principles to facilitate and protect the flow of personal data in the market.

Among the key changes (see figure 1), organizations must prove that they have a robust accountability framework in place for data protection, an ongoing data protection impact assessment and a privacy-by-design approach. The latter ensuring that data protection safeguards are built into products and services from the earliest stage of development. Key rights for individuals include the right to erasure (right to be forgotten), and the requirement for consent to be explicitly given for specific uses and transfer of sensitive data.

GDPR key changes

Figure 1

A monumental impact

Although GDPR brings a welcome harmonization of fragmented data protection laws across EU Member States, its wide-reaching impact and stringent rules require a fundamental organizational shift, even for businesses compliant with existing legislation. When the steep financial penalties for non-compliance and data losses are added to the cost of reputational damage, sanctions, remediation and the potential impact on digital transformation, the risk of inaction is clear.

> … its wide-reaching impact and stringent rules require a fundamental organizational shift.

Start with assessment

The first step to GDPR readiness is to understand and assess current privacy maturity and data flows across the organization. As business models have digitized, the volume and spread of personal data held and used by organizations has increased significantly. Many struggle to understand how much data they hold, why they retain it and how it is being used across thousands of applications and the full personal data life cycle.

Given the scale and complexity of the GDPR challenge, achieving timely compliance requires more than a tick box gap analysis and remediation exercise. By taking a strategic, risk-based approach to GDPR readiness, organizations can achieve both compliance and competitive advantage.

Personal data life cycle management

A strategic approach to GDPR compliance and beyond

The drivers for data protection and privacy compliance are clear (see figure 2). However, increasingly, data protection and privacy are not just compliance issues. But instead, they directly impact many areas of business operations.

The wide-reaching impact on business means data protection and privacy becomes a factor in business strategy and should form part of the management agenda. As a result, organizations can use GDPR as a catalyst for change beyond compliance, from enhancing reputation and customer loyalty, to digital transformation, meeting stakeholder expectations and delivering the broader change agenda. See figure 3 for further strategic incentives.

Figure 2

Compliance incentives

- Need to comply with laws, regulations, contracts and other agreements
- Increasing pressure from regulators
- Minimization of reputational damage
- Rising fines and penalties
- Significant costs associated with recovery from breaches and potential lawsuits

Figure 3

Moving beyond compliance – strategic incentives

- Treat privacy as one of the key drivers to enhance brand and reputation
- Ensure privacy and trust while the added value of new digital propositions are realized
- Continue to enable big data and predictive analytics, and have them comply with the privacy regulation
- Protect data and privacy in the complex eco system
- Meet stakeholders' expectations, especially in light of increasing public awareness of and concern about data privacy
- Include data protection and privacy as ethical responsibility toward customers (building a better working world)

It's time to take ownership of data and privacy governance

Personal data is increasingly valuable

Organizations today collect a large volume of data, much of which can be personal information that could identify individuals. This data is an increasingly valuable asset, providing the backbone for market and client insight, product and service offerings, and day-to-day operations, particularly as organizations extend their digital proposition and business model.

A tailored journey

A one-size-fits-all approach to GDPR readiness is likely to fail. Organizations will have to take ownership of their data and privacy governance. While the business value of data protection is clear, it is equally important to understand each organization's unique balance of risk appetite, organizational infrastructure and privacy maturity. This sets the foundation for developing an effective, tailored GDPR road map and implementation program.

Taking a prioritized approach

We believe taking a risk-based approach enables organizations to develop a customized road map that prioritizes investment in the higher risk and high-value data flows and systems that matter most to their business.

Multi-disciplinary governance

Even with a tailored, prioritized plan in place, operationalizing the new framework and remediating legacy systems and processes across the organization is a complex challenge that requires the collaboration of many disciplines.

The cross-functional nature of the impact of GDPR means establishing effective multi-disciplinary governance early on is fundamental to success. Where previously privacy and data protection could be seen as simply an IT or legal issue, they now require active engagement from a wide range of functions, including business operations, vendor management, legal, risk, HR, IT security and data management.

EY multi-disciplinary transformation approach

Our broad transformation approach mirrors the cross-functional nature of the GDPR.

We bring our own multi-disciplinary team of professionals, combining knowledge and experience across legal, cybersecurity and data analytics, to engage with stakeholders from all parts of the organization, to bring GDPR to life.

Our five-phased approach (see figure 4) is a framework from which we can build a tailored approach for each organization, to operationalize GDPR, and provide compliance and beyond.

Figure 4

1. Understand

The business and governance models

Gather information related to the organization and its adopted strategies to understand the current data protection governance model. Assess the industry and market, the organization's management structure and its digital and data strategy, as well as the data protection measures and awareness in place.

Data protection and privacy framework

Leverage acknowledged frameworks, gather information and create an understanding of the existing data protection and privacy posture of the organization, including policies, standards and guidelines.

Legal and regulatory framework

Understand the organization's status and compliance toward the applicable laws and regulations, specifically GDPR and sector-specific laws and regulations.

Data transfers with vendors and partners

Understand the organization's vendors and partners, including providers of cloud services and outsourcing. Create an overview of data transfers abroad, and understand the legal and regulatory impact.

2. Assess

Strategic alignment and risk appetite

Determine the strategic alignment and risk appetite in a workshop. Define the "tone at the top" toward strategy, risk culture, direction and conduct.

Data flow mapping

Map data flows to enhance the implementation support of data privacy. The identified data streams can be used to determine the requirements for privacy (on the basis of applicable laws and regulations) and setting up data protection.

GDPR maturity assessment

A tool-based privacy questionnaire is developed to assess the privacy maturity in different privacy domains, such as privacy strategy, data classification, etc.

Road map

The road map contains the necessary actions identified during the assessments and workshops. It will focus on compliance toward the applicable laws and regulations, and the defined privacy and data protection strategy.

3. Define

Privacy and data protection strategy

Develop an overarching strategy aligned with the business strategy and identified process improvements.

Governance, policy, standards and guidelines

Redefine the data protection governance model, including a detailed description of the roles and responsibilities with regard to management of external relationships and communication with regulators.

Data usage and flow mapping

Create an overview of where sensitive data flows within the organization. Develop a data usage model based on legitimate use and consent as well as sustainable registration.

Data subject rights

Define processes to ensure data subject rights are enforceable. Facilitate compliance through privacy by design, e.g., embed user access rights in online applications. Evaluate and redesign processes for retrieval, correction and erasure of personal data throughout the organization.

Data protection impact assessment and privacy by design

Assess personal data collection and processing activities with a data protection impact assessment to identify the risks inherent to the personal data processing activities. Reduce such risks by redefining the processes in accordance with the principles of privacy by design and privacy by default.

Vendor and partner management

Identify and prioritize the vendor relationships, which include personal data processing activities. Evaluate the contracts, security measures and oversight governance against compliance with GDPR and define a strategy to renegotiate personal data processing agreements. Ensure appropriate security measures and vendor management are in place by defining a lean oversight governance.

Monitoring and incident handling

Define a process for personal data breach monitoring and reporting. Develop a process for personal data breach reporting toward the data protection authority and toward the data subjects. Design templates and communication approval processes to ensure that the notification deadline of 72 hours can be met.

4. Recommend

Recommend the processes and measures defined in the previous phase 3, by leveraging existing processes within the organization. Ensure data protection governance and documentation are in place by introducing internal guidelines and process documentations in order to comply with the accountability principle.

5. Run

Privacy control framework

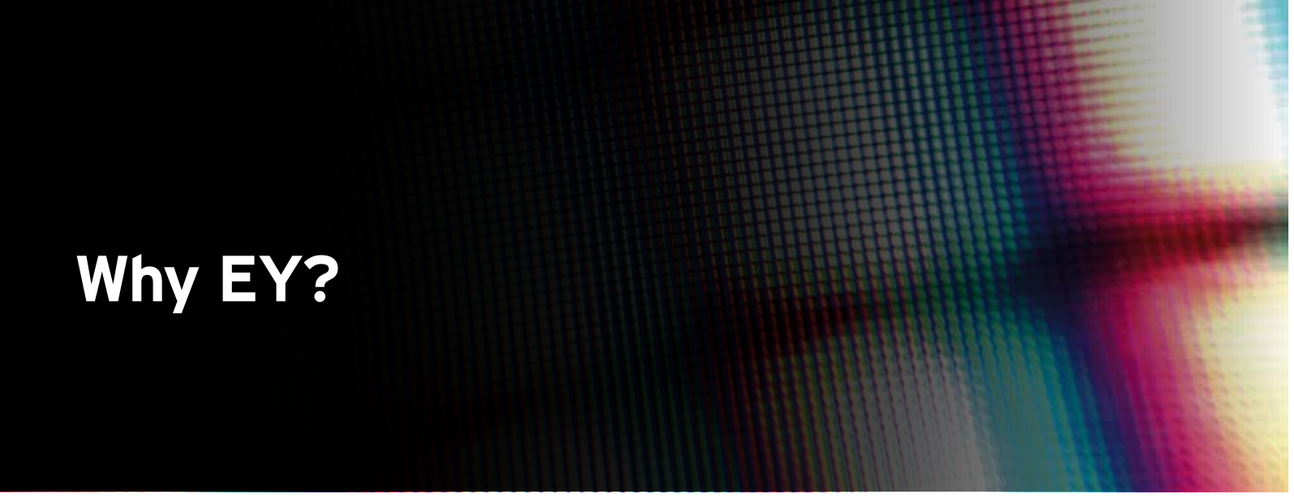
Facilitate compliant personal data management through a holistic privacy control framework, integrating data protection throughout the organization, including project management, process and product development, as well as risk and vendor management.

Raising awareness

Ensure data protection and privacy awareness through appropriate information, and specific data protection awareness trainings and workshops. Workshops will help stakeholders to understand that privacy is more than solely a compliance or security issue. Privacy game, case study and break out sessions form a part of the awareness workshops.

EY can help with managed services

- Web-based data protection trainings
- Data protection impact assessments
- Compliance monitoring
- Data breach stress tests



Why EY?

1. Extensive privacy knowledge and experience

EY employs over 200 Certified Information Privacy Professionals (CIPPs) and privacy lawyers to help organizations to better understand data privacy risk and GDPR compliance. Close cooperation with EY legal specialists means EY CIPPs can translate legal requirements into a risk-based, customized approach.

2. Global teams

EY teams work within common global structures so they can easily draw on EY's global industry and functional experts to bring insights on legislation, regulations and business practice across the globe. EY has proven success in rollout across multiple countries.

3. Highly experienced

For over a decade, EY has assisted multi-national organizations in understanding privacy and data protection and regulations such as GDPR. Using their deep industry and client knowledge, EY has helped clients across financial services achieve both compliance and competitive advantage through effective GDPR programmes, from gap analysis through to ongoing managed services.

4. Professional approach

EY uses a risk-based, multi-disciplinary approach supported by robust tools and methodologies to help you to understand the impact of GDPR on your organization, achieve timely and consistent GDPR compliance and leverage GDPR for wider strategic benefit.

EY Contacts

To discuss how EY can help you use GDPR as a catalyst for change, beyond compliance, please contact:

Erol Mustafa
EMEIA Financial Services IT Risk & Assurance Leader

Telephone: +44 20 7951 0700
Mobile: +44 7979 923611
Email: emustafa@uk.ey.com

Philippe Zimmermann
EMEIA Financial Services Legal Leader

Telephone: +41 58 286 3219
Mobile: +41 79 341 4571
Email: philippe.zimmermann@ch.ey.com

Tony De Bos
EMEIA Financial Services Data Protection & Privacy Leader

Telephone: +31 88 407 2079
Mobile: +31 62908 4182
Email: tony.de.bos@nl.ey.com

Konrad Meier
EMEIA Financial Services Data Privacy Professional

Telephone: +41 58 286 4327
Mobile: +41 79 227 2367
Email: konrad.meier@ch.ey.com

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 financial services industry
We understand the importance of asking great questions. It's how you innovate, transform and achieve a better working world. One that benefits our clients, our people and our communities. Finance fuels our lives. No other sector can touch so many people or shape so many futures. That's why globally we employ 26,000 people who focus on financial services and nothing else. Our connected financial services teams are dedicated to providing assurance, tax, transaction and advisory services to the banking and capital markets, insurance, and wealth and asset management sectors. It's our global connectivity and local knowledge that ensures we deliver the insights and quality services to help build trust and confidence in the capital markets and in economies the world over. By connecting people with the right mix of knowledge and insight, we are able to ask great questions. The better the question. The better the answer. The better the world works.

EYG No. 05461-174Gbl
ED None

ey.com/fs