Can compliance help you compete?

Helping technology, media and telecoms companies succeed with the EU General Data Protection Regulations

The better the question. The better the answer. The better the world works.
Contents

Introduction 1

Tip 1: Keep up-to-date with evolving regulatory guidance 3

Tip 2: Establish a GDPR implementation program – deploying a multidisciplinary approach 6

Tip 3: Prioritize the elements of your GDPR program to align with business critical requirements 12

Tip 4: Look beyond the deadline date of 25 May 2018 14

EY and GDPR – a successful combination 16

ey.com/uk/tmt
Twitter @EY_TMT_UK
The role that technology, media and telecoms (TMT) companies have as custodians of high volumes of consumer data, will make them among those most affected by EU General Data Protection Regulation (GDPR).

Recent high-profile breaches of customer data underline the reputational risks facing TMT companies in the digital era, as consumer concern around the integrity and security of their personal data continues to rise. The burden of effective data storage and management remains pronounced, and personal data is at the heart of TMT companies’ current and future business models. As such, GDPR’s impact will extend beyond operational areas into strategic ones. A successful GDPR program must therefore meet complex regulatory requirements while also sustaining wider business objectives allied to increased customer centricity.

The opportunity around GDPR can be summed up in one word – trust. If personal data is the lifeblood of TMT businesses, then the companies that consumers feel most able to trust with that data will have a competitive edge. Looking ahead to areas such as the connected home, the value of that trust is only likely to grow. GDPR therefore creates an industry-wide opportunity to build and communicate new standards for consumer rights in terms of data. Successful companies will seize that opportunity with strong compliance systems that protect against the financial and reputational damage of regulatory breaches.
Can compliance help you compete?

About the new regulation

GDPR was designed with two main objectives. First, it is designed to protect consumer and individual rights. Second, it gives businesses a simpler, clearer legal environment in which to operate, making data protection law identical throughout the European Single Market.

For the regulators to be able to achieve these twin objectives, companies must meet a number of new requirements (see figure below) and be ready to comply by 25 May 2018, or face fines of up to 4% of turnover.

This combination of an impending deadline and the risk of severe financial penalties is understandably focusing the minds and resources of TMT companies. But it is important to remember these are only the headlines in a story that will have far-reaching implications for the sector.

To be successful, your compliance program must therefore be about more than meeting tough deadlines and avoiding penalties. It must satisfy not only the regulator’s requirements, but also those of your customers, investors and employees.

Achieving that success means drawing on a combination of commercial, sector, legal and data privacy expertise to design the right GDPR solution for your business. EY’s risk-based, multidisciplinary 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.

In this report, we outline the four key tips for your GDPR program.

### Fines
Up to 4% of the annual worldwide turnover or over £20 million, whichever is greater

### New rights
- Right to be forgotten
- Right to data portability
- Right to object profiling

### DPO
Data protection officer must be appointed if an organization conducts large-scale systematic monitoring or processes large amounts of sensitive personal data

### Consent
Must be explicit and clear for specific purposes

### Privacy impact assessments (PIA)
Organizations must undertake PIA when conducting risky or large-scale processing of personal data

### Accountability
Is the key of getting it right today and beyond 25 May 2018

### Privacy by design
Organizations must design data protection into the development of business processes and new systems. Privacy settings are set at high level by default

### 25 May 2018
Organizations need to get ready by the deadline
Comply, demonstrate, repeat

One lesser-known aspect of the GDPR Regulation (EU) 2016/679 is that the word “demonstrate” appears no fewer than 26 times. This is no accident – it is there to indicate new expectations of accountability. Businesses must be able to demonstrate that appropriate actions have been taken in accordance with the regulation.

Keep track as the new regulation beds in

The detail on areas such as exactly how businesses demonstrate compliance and the criteria by which this will be assessed may not have been fully resolved before the May 2018 deadline.

Just as, for the past 12 months, there have been dialogues and interactions between the business and data protection authorities in relation to technical guidance on GDPR, this is expected to continue beyond 25 May 2018. Overall, this should have a positive impact as consultation and engagement with other sector-specific regulators and data protection authorities, will provide a useful way of resolving any outstanding issues and ensuring that business and marketplace are aligned. But businesses will need to keep track of this and take advantage of any refinements that could benefit their GDPR processes.

Tip 1: Keep up-to-date with evolving regulatory guidance

Success is not only complying, it is being seen to have the processes in place to ensure compliance.

Success is being aware of and engaged with evolving regulation.

Helping technology, media and telecoms companies succeed with the EU General Data Protection Regulations
Look for opportunities to harmonize

Organizations are likely to welcome the harmonization of laws across the 28 Member States, but an awareness of national differences may still be essential.

Under the current EU Data Protection Directive, the Article 29 Working Party (Art. 29 WP) plays a leading role in ensuring a consistent and EU-wide approach to data protection. Representatives from each EU data protection authority meet regularly and make recommendations to the public. These powers will be further strengthened by the European Data Protection Board (EDPB), which will replace the Art. 29 WP under GDPR.

This combination of mutual collaboration and unified regulation is designed to drive the shift from an environment where each of the EU’s 28 Member States has a distinct regulatory enforcement approach to one where laws are harmonized.

While this will make the complex data protection landscape easier to navigate for multinational organizations, businesses must be aware that the shift to coordinated enforcement will be gradual.

Here, EY is strongly placed to support clients because of our experience in and engagement with public consultation and policy discussion with EU institutions, data protection authorities and sector-specific regulators.

Handle with care – TMT’s sector sensitivities

GDPR will have a greater impact on organizations that, like many telcos and media companies do, deal with large numbers of end customers. Potentially every customer can submit a Subject Access Request (SAR) to, for example, erase personal data and object to marketing emails. To satisfy regulators, data controllers need to respond to these requests, no matter the volume, within a defined timeline.

Telecoms providers in particular need to form a unified (or consistent) position on how to respond to call data record (CDR) data portability requests, and decide if they should deviate from opinions issued by Art 29 WP and the Information Commissioner’s Office (ICO). Organizations must also be prepared to respond to requests from individuals who want to exercise their rights about the processing of their personal data. As well as businesses who are using data processors to process their commercially sensitive information, and requests or investigations from Supervisory Authorities (SAs).
Take a forensic approach to cybercrime

The days when some companies quietly swept cybercrime-related data breaches under the carpet are over. Under GDPR, organizations will have to inform the regulators of data breaches “without undue delay and not later than 72 hours after becoming aware of it.”

TMT companies must put processes in place to identify and contain a breach, to assess the risk to individuals, and then to determine whether it is necessary to notify the competent supervisory authority or the individuals concerned.

The first stage is detection and here cybercrime forensics skills will be needed as part of any successful GDPR plan. EY’s forensic investigation team engages with multinational TMT businesses around the world to help prevent and detect fraud, enabling us to have a global view of trends and incidents. We can help companies protect themselves and their customers against an array of techniques from pre-texting and social engineering to hacking and “spof” emails. We can also help through incident and investigation response, performing vulnerability assessments, developing processes to safeguard critical information, and increasing awareness of current fraud trends.

EY and the regulators – valuable experience

We engage with regulators across the world, both to clarify individual client issues and play a part in shaping industry-wide regulation. This experience can be valuable during GDPR planning, design and implementation.

Pragasen Morgan
Privacy Leader, Ernst & Young LLP
pmorgan@uk.ey.com

Trevor Horwitz
Fraud Investigation & Dispute Services (FIDS) Partner, Ernst & Young LLP
thorwitz@uk.ey.com

Ian Williamson
Head of Digital and Privacy Law, Ernst & Young LLP
iwilliamson@uk.ey.com
Twitter: @IanWTechLaw
Can compliance help you compete?

Tip 2: Establish a GDPR implementation program – deploying a multidisciplinary approach
GDPR implementation is a compliance exercise that will affect multiple business departments and functions across several countries. Delivery responsibilities need to be clearly identified and collaboration with stakeholders established at a very early stage.

To achieve this, people, processes and technology within your organization need to work together across departments and geographies. In our experience of working with TMT companies, these are the key factors that will support this objective.

**Take a multidisciplinary approach**

The cross-functional nature of GDPR means that establishing effective multidisciplinary 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. The deliverables, design and implementation timelines and key responsibilities need to be agreed, for example, with:

- Technology, which may also provide concepts or tools for data pseudonymization and anonymization, and data registers
- Security, which must review their data-breach management process, and ensure that security by design is incorporated in the future
- HR, which must review and update privacy notices, consent and rights of employees
- Sales and marketing, which must review and update existing contracts and processes
- Other departments, such as procurement or the data centers, which must review contracts and their existing processor-controller relationships

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’s legal professionals means EY CIPPs can translate legal requirements into a risk-based, customized approach.

**Secure senior management sponsorship**

A robust governance framework for GDPR should flow from the top down. Global organizations need to appoint a steering committee (SteerCo) that provides oversight and enables fast-track decision-making for headquarters and group functions. Cross-organizational SteerCo stakeholders should be invited to regular meetings, and escalation procedures need to be defined. If the organization has offices in many countries, the same governance structure should be applied to ensure a consistent roll-out of GDPR in all countries that are in scope.
Agree a reporting structure and assurance plan

Successful implementation means developing a robust reporting framework. This should consist of a qualitative part, which gathers monthly information on what has been achieved, activities planned, and issues and risks; and a quantitative part, which implements red-amber-green (RAG) ratings or maturity ratings that can be translated into heat maps and diagrams for management presentations.

In the final stage and/or after implementation, independent testing by internal audit or a third party must be carried out. An assurance plan that outlines the scope, objectives and testing approach must document how assurance over the implementation was obtained.

Clearly define GDPR deliverables

Organizations have been complying with existing EU data protection directives for some time, so what is needed now is to identify which GDPR requirements apply to your organization and which will require new deliverables.

These may include:

- Identification of high-risk processing activities
- Conducting privacy impact assessments (PIAs)
- Incorporating the precept of privacy by design into products, services and operations
- Tightening the regime of managing permissions, transparency and privacy notices
- Expanding individual rights to include “the right to be forgotten” and data portability
- The capability to notify the regulatory authority within 72 hours
- Changing the processor-controller relationship

Can compliance help you compete?
Helping technology, media and telecoms companies succeed with the EU General Data Protection Regulations
TMT hot topics

GDPR presents the TMT sector with specific challenges. Addressing these in a way that satisfies regulators while achieving business objectives is key to successful GDPR compliance.

Consents and permission
When a customer signs a contract for the whole family, how is consent managed, especially when children are involved?

Data analytics
Most organizations use customer data to get vital intelligence for their business model and marketing activities. However, unless this data is effectively depersonalized it will not be GDPR-compliant.

Subject access requests
GDPR is designed to empower data subjects and gives them additional rights. These include access (Art 15), rectification (Art. 16), erasure (Art 17), restriction of processing (Art. 18), data portability (Art 20), object to use (Art 21) and restrictions on automated decision-making (Art 22).

Develop a central consent and transparency system, which stores relevant information and allows individuals to, through a self-managed portal, carry out updates/changes to their consent profile.

Build your capabilities so that you can effectively depersonalize consumer data before using it for analytics.

Make sure your GDPR program is capable of validating these requests then responding to them quickly, accurately and cost-effectively.
Helping technology, media and telecoms companies succeed with the EU General Data Protection Regulations
While the intention of GDPR is to make EU data privacy regulation uniform across different sectors and countries, this does not mean compliance processes and strategies are universal.

Far from it, a one-size-fits-all approach to GDPR readiness is likely to fail. Only by understanding each organization's unique balance of risk appetite, organizational infrastructure and privacy maturity can the foundations be laid for an effective, tailored GDPR program. Prioritization will be key.

Only high-risk personal data processes, products and services are in scope of the new regulation so mapping all personal data processes and identifying all data flows is unnecessary and is likely to prove a waste of time and resources.

**Create a risk-based GDPR program**

The process should begin with a risk assessment. Every organization is different but privacy risks faced by many larger TMT businesses include:

- Reputational risks that can be caused by data leakage
- Inappropriate usage of personal data by big data analytics
- Personal data storage and processing by shared services centers (within and outside the EU) or in the cloud
- Insufficient consent by data subjects to the use of their data by third parties for marketing or sales activities

Our multidisciplinary approach is supported by robust tools and methodologies to help you understand the impact of GDPR on your organization, achieve timely and consistent GDPR compliance and leverage GDPR for wider strategic benefit.

**Tip 3:**

Prioritize the elements of your GDPR program to align with business critical requirements
Our combined forensics and legal service translates the core requirements into a risk-based, customized approach and provides you with a single service provider to collaborate with in your GDPR transformational journey.

**Bring data and stakeholders together across your organization**

We understand the challenges embarking on a GDPR program entails, from involving the right stakeholders, to understanding the flow through structured and unstructured data and educating senior management on the impact GDPR will have on business-as-usual activities.

We bring these insights together with our tools and accelerators to provide a successful assessment and program definition. Our insights will help with the continued enhancement and improvement of your program along with the lessons we have learned from our work with other large organizations.
While deadlines are a highly effective way of focusing minds and providing a clear common objective, the reality is that 25 May 2018 is not the finishing post. Successful GDPR programs will continue to develop and adapt as regulations, markets and technology continue to evolve.

For example, an individual’s “right to data portability” is a key challenge for organizations, as they must enable individuals to transfer personal information to another “data controller.” Here, there will be an opportunity for the TMT sector to revisit current technical guidance and provide feedback for improvement.

**Become a thought leader, not a follower**

As businesses implement and apply their GDPR processes, lessons will be learned and new thinking and methods will evolve. Staying connected through both public forums and your EY advisors will help you to develop your methodology and improve outcomes.

To support this, we regularly host client forums and produce surveys to help understand the key trends, current challenges and the future direction of privacy. We recently published the Annual Privacy Governance Report in association with the International Association of Privacy Professionals (IAPP).

One current trend is the shift to plan audit and assurance GDPR implementation program by focusing on project governance, accountability and prioritized work streams. To maintain a privacy compliance framework, it is important that regular independent assurance through desktop or more substantive audits is carried out. These should take place at least on a monthly basis.
Look beyond the deadline to think sustainably
Successful businesses think long term, so GDPR solutions should be built to last. That means creating a sustainable program that not only works toward current business objectives but is also flexible and scalable enough to enable future change and growth.

Don’t keep privacy private
GDPR compliance should not be seen in isolation. Its principal subject, data, clearly connects it to critical areas such as cybersecurity and data protection. A new, collaborative model is needed to unite the multiple dimensions of privacy within the organization.

The value of this approach is increased by the fact that data protection and privacy are a factor in business strategy. As a result, organizations can use GDPR as a catalyst, from enhancing reputation and customer loyalty, to digital transformation, meeting stakeholder expectations and delivering the broader change agenda.

EY is ideally placed to support this as we have been providing privacy and data protection change programs for over ten years, supported by over 200 certified information privacy professionals (CIPP).

We work with regulators on this topic and are approved under binding corporate rules (BCRs) to transfer personal data cross border, globally, by the ICO.

Put trust at the heart of your approach
As technology becomes integral to ever more aspects of everyday life, the need for customers to trust organizations with their data is increasingly important. As TMT companies typically hold personal information such as location, name and age, for both adults and children, the need to earn, maintain and safeguard that trust is essential. By being seen to not only comply with the letter but also the spirit of GDPR, TMT companies have an opportunity to differentiate themselves as champions of consumer rights in the digital age.

This can be achieved by clearly communicating your commitment to customers, providing greater transparency about their rights and offering simple, easy-to-use interfaces for consumers to self-manage data consent, portability and erasure.
EY has proven success across multiple countries of:

- Providing large and complex regulatory change programs, encompassing security, privacy and risk
- Advising some of the world’s largest TMT organizations on all aspects of data protection and privacy
- Assisting significant GDPR programs

EY and GDPR – a successful combination

We are helping clients across the TMT sector to achieve compliance and gain competitive advantage through effective GDPR programs. Our multidisciplinary teams translate core legal requirements into a risk-based, customized approach, acting in close cooperation on your GDPR journey.

EY’s approach

- **Broad** in reach through its four phases: understand, assess, design and assist
- **Multidisciplinary** by integrating the legal, IT, risk and business perspectives of privacy
- **Single EY legal and advisory** privacy offering to translate legal requirements into risk-based, customized approach
- Identification of pragmatic, **realistic and risk-based** remedial implementation options for **GDPR readiness**
## Getting ready for GDPR — how we can help you prepare

<table>
<thead>
<tr>
<th>Category</th>
<th>Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>GDPR assessment (targeted and 360-degree)</td>
<td>- High level assessment of data protection maturity</td>
</tr>
<tr>
<td></td>
<td>- Detailed assessment of data protection maturity</td>
</tr>
<tr>
<td></td>
<td>- Compliance requirements</td>
</tr>
<tr>
<td></td>
<td>- Risk assessments</td>
</tr>
<tr>
<td>Privacy impact assessment</td>
<td>- Customized privacy impact assessment</td>
</tr>
<tr>
<td>“Know your personal data” — data inventory</td>
<td>- Personal information inventory</td>
</tr>
<tr>
<td></td>
<td>- Personal information flow documentation</td>
</tr>
<tr>
<td>End-to-end GDPR implementation program</td>
<td>- Program design</td>
</tr>
<tr>
<td></td>
<td>- Program implementation</td>
</tr>
<tr>
<td></td>
<td>- Compliance and monitoring solutions</td>
</tr>
<tr>
<td></td>
<td>- Ongoing program support</td>
</tr>
<tr>
<td></td>
<td>- Customized training and workshop</td>
</tr>
<tr>
<td></td>
<td>- Prioritized GDPR work streams</td>
</tr>
<tr>
<td></td>
<td>- PMO coordination, reporting and support</td>
</tr>
<tr>
<td></td>
<td>- Coaching and training</td>
</tr>
<tr>
<td>Legal support</td>
<td>- Legal analysis</td>
</tr>
<tr>
<td></td>
<td>- Drafting of legal documents</td>
</tr>
</tbody>
</table>
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.

© 2017 EYGM Limited.
All Rights Reserved.

EYG no. 06657-174Gbl

ED None

In line with EY’s commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

ey.com/UK