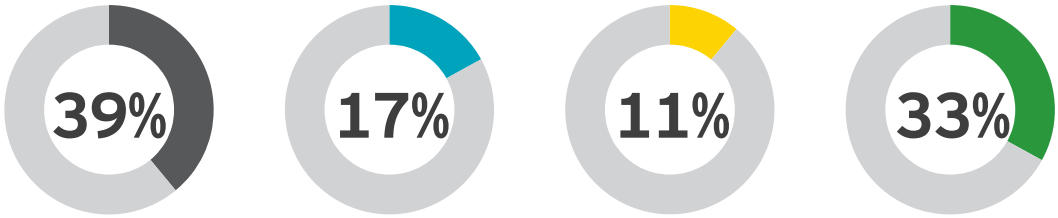
GDPR compliance – from planning to action

Companies worldwide raced to complete General Data Protection Regulation (GDPR) compliance plans before the regulation's effective date, 25 May 2018. However, a recent global survey conducted by EY shows that a large number of companies may still not be ready now that the deadline has passed.

According to the *EY Global Forensic Data Analytics Survey 2018*, only 33% of respondents had a compliance plan at the time of the survey (October and November 2017). Another 11% were working toward compliance. An astounding 56% were either unfamiliar with GDPR or had not yet taken any action. Needless to say, planning and preparation is continuing after 25 May for those particular respondents.



Source: EY Global Forensic Data Analytics Survey 2018

Even for those who have a compliance plan in place, the journey is not over. GDPR compliance cannot be achieved through a "one-and-done" compliance exercise. Achieving compliance requires ongoing due diligence by companies to effectively manage compliance risk. Having a plan is one thing; being able to effectively prove to a supervisory authority that the company has a compliant program in place can be as challenging. It requires continuing evaluation of the planned procedures and processes, and fine tuning based on compliance results and the changing business and risk environment.

What companies are facing post-25 May

Supervisory authority inquiry

Companies could be subject to supervisory authority inquiry of potential violations of certain GDPR requirements. The process to respond to the inquiry can be complicated. It can involve extensive communication or negotiation with one or more supervisory authorities; it can also require companies to conduct internal investigations.

Data mapping and data governance

To meet GDPR requirements, companies need to map the personal data of EU data subjects that they process, and to ensure that it is processed appropriately and it is adequately protected. Data governance frameworks supported by appropriate policies and technology are needed to make sure GDPR compliance is achievable and sustainable in the long run.

Data subject access requests

The GDPR grants data subjects several core rights to access and control their data (e.g., "right to be forgotten"). A well-designed compliance plan with appropriate workflows should enable a company to respond to subject access requests within the prescribed time requirement, which is generally 30 days barring special circumstances. However, there will be times when the response or lack of a response leads to a dispute. In those cases, the company may be obligated to take further actions, such as electronic discovery, to prove the completeness of its response or to uncover the data it wasn't able to locate as required.

Data breach response

The GDPR requires supervisory authorities be notified, under certain circumstances, within 72 hours of a personal data breach. Companies need to achieve a basic level of understanding of the scope of the breach to determine the appropriate notification procedures. Conducting a swift breach investigation is therefore critical to meeting the GDPR breach notification requirement. Having a GDPR compliance plan that works in conjunction with the company's cyber breach response plan will enable the company to respond to the breach in an effective manner within the short time window available to do so.

Data privacy assessment (DPA), training and governance

Companies will have an ongoing need to conduct a DPA as new systems are implemented, new data sources are used or analytics are developed. A key component of GDPR transformation is changing the behaviors of employees. Companies need to develop tailored data privacy training to support the specific needs of employees who handle personal data. In addition, companies will be required to maintain a defensible position around all of their GDPR obligations. They therefore need to capture key data privacy management artifacts in a central place to support regulatory inquiries.

Data protection officer (DPO)

A DPO will need an understanding of data protection law and practices, IT infrastructure, cybersecurity and training, and be free of conflicts of interest. The GDPR allows for an external DPO, and some companies will determine that approach makes sense. Where a specific expertise is scarce, companies will likely need to look for outside help.

EY contacts

EMEIA

- Meribeth Banaschik
  meribeth.banaschik@de.ey.com
- Ryan Rubin
  ryan.rubin@uk.ey.com
- Tony de Bos
  tony.de.bos@nl.ey.com
- Fabrice Naftalski
  fabrice.naftalski@ey-avocats.com

Americas

- Eric Schwarz
  eric.schwaz@ey.com
- Todd Marlin
  todd.marlin@ey.com
- Angela Saverice-Rohan
  angela.savericerohan@ey.com

Asia-Pacific

- Reuben Khoo
  reuben.khoo@sg.ey.com
- Jeremy Pizzala
  jeremy.pizzala@hk.ey.com

Japan

- Ichiro Sugiyama
  ichiro.sugiyama@jp.ey.com
- Izumi Umezawa
  izumi.umezawa@jp.ey.com

For a complete listing of our GDPR-related thought leadership, please go to: ey.com/GDPR.

How EY can help[1]

We can help companies mitigate risks and protect shareholder value by proactively managing the response to GDPR requirements. EY GDPR services are joint efforts of service professionals from the fields of advisory, data privacy, forensics, IT, cybersecurity, corporate governance and law. We combine our interdisciplinary teams and the client's cross-functional stakeholders for one detailed approach.

Supervisory authority inquiry

- Investigation
- Risk remediation
- Legal advisory

Data mapping and data governance

- eDiscovery
- Information governance strategy
- Data management program development

DPO managed services

- Internal communication and training
- Communication with supervisory authority
- Responding to data subjects' requests
- GDPR compliance reporting and monitoring

Data breach response

- Cyber breach preparation
- Cyber breach response management
- Cyber investigation and triage
- Crisis risk management

Data privacy assessment and training

- Compliance program assessment
- Data privacy laws
- Mock regulatory audits
- Data privacy awareness program
- Data privacy training

[1] EY does not provide legal services in the US.

EYG no. 03879-183GBL
CSG no. 1802-2594897

ED None.