Introduction

The General Data Protection Regulation (GDPR) is ushering in a new era of data privacy in Europe.

Organizations that want to assess maturity or demonstrate robust privacy to their stakeholders need the assurance of an independent, professional opinion.

EY’s data privacy assurance services offer a range of approaches that can be tailored to the needs of every client.
GDPR and the privacy agenda

Organizations around the world face a revolution in data privacy. Regulators in many markets are enforcing existing privacy regulations more actively than in the past, and jurisdictions, including the US, are introducing strong new data privacy laws.

Europe’s GDPR entered force in May 2018. First proposed in 2012, the GDPR applies uniformly across the EU and affects any organizations, not just those collecting personal data.

The effects of the GDPR are far-reaching. Other EY research explores this in detail and can be found at ey.com/fsgdpr. But, for commercial organizations, the most important points are:

- GDPR imposes significant responsibilities in areas, such as documentation, reporting, governance and product design.
- It applies to organizations designated both as data controllers (those that determine how and why personal data is used) and data processors (those that collect, organize, store, use or disclose data on behalf of controllers), regardless of contractual relationships.
- It allows for fines of up to €20m or 4% of global revenues, whichever is the highest.

Furthermore, the GDPR is only one driver of the privacy agenda. Consumer awareness of data privacy risks are growing rapidly across Europe. As customer expectations rise, organizations are realizing that demonstrating effective data privacy is critical to building customer trust.

This combination of drivers means that many companies now view data privacy as a strategic goal, not just a compliance target. The ability to demonstrate robust data privacy could soon become a source of competitive advantage in many markets.
GDPR challenges and how EY can help

Organizations that want to demonstrate their compliance with the GDPR first need to ensure that they meet its requirements. In practice, many organizations are finding this a challenging goal and some have a significant distance to go. EY offers a range of services, including a detailed privacy transformation program, to help organizations comply with the GDPR.

When it comes to demonstrating clients compliance with the GDPR, EY’s data privacy assurance services give clients independent assistance about their data protection controls. The benefits of data privacy assurance include:

- Indicating compliance to supervisors and other external stakeholders
- Showing that organizations have implemented processes to protect personal data
- Demonstrating that organizations execute procedures to limit the possibility of a data breach

The four services that support achieving these benefits are performing a GDPR maturity assessment, GDPR Certification, International Standards on Assurance Engagements (ISAE) 3000 and Service Organization Control (SOC 2) reporting. Although these are not mutually exclusive, deciding which service an organization requires depends partly on which GDPR category it falls into (see graphic).

---

What does your organization need?

Organization wants to demonstrate GDPR compliance

Assessment of privacy procedures
Certificate without details for external use; Report with details per criteria for internal use

Identification of current gaps in relation to GDPR requirements
Conformity assessment with regard to criteria comparable to GDPR regulation

Organization should request this type of opinion:

Internal need
GDPR maturity assessment

External need
GDPR Certification

Report needs to include assurance

Limited time and/or experience with SOC 2

Transparency (based on the defined criteria)

Opinion over privacy controls
Opinion over privacy processes and controls

ISAE 3000
SOC 2

External need

Demonstrating data privacy for GDPR and beyond EY data privacy assurance services
**Client challenge:**
The business has an internal or external need to demonstrate the quality of its implemented privacy processes without detailing its complexity.

**How EY can help:**
EY can perform a GDPR maturity assessment within your organization, which is a comprehensive in-depth assessment covering multiple privacy domains. The assessment provides insight in the maturity of the organization and identifies gaps. For each domain, the current situation is identified based on GDPR requirements, gaps are identified including the risks and a prioritization to resolve the gaps.

**Client challenge:**
The business has an internal need to demonstrate the maturity of its privacy processes.

**How EY can help:**
EY can provide the business with GDPR Certification which reviews conformity to the requirements in the GDPR via a set criteria and is reported through a Certificate and a separate report. It demonstrates that the business's privacy processes have been audited and the report includes details of how conformity has been assessed to the criteria established. The reports are primarily for internal use and can be shared with regulators if needed. Certificates are valid for a period of three years and can be displayed to the public. Once GDPR compliance has been achieved, certification is typically a relatively quick and straightforward process.

**Client challenge:**
The business has an external need to demonstrate or disclose the implementation of privacy processes and the operating effectiveness of the controls in these processes.

**How EY can help:**
EY can audit the design and operating effectiveness of the privacy processes. There are several auditing standards which can be used to provide assistance in the privacy processes.

**ISAE 3000 Report (Third-Party Memorandum):** EY can provide a proprietary control framework to be accustomed to the organization's own processes. This enables the audit activities to be performed on agreed criteria on the organization's implemented privacy controls and to conclude on these controls effectiveness.

**SOC 2 Report:** A SOC 2 contains a full description of your internal processes and the business’s data privacy controls. It is a rules-based set of criteria, which at minimum have to agree back to commonly accepted set defined by the accounting board. With its implementation, an EY SOC 2 opinion can still be tailored to the organization's requirements, demonstrating to stakeholders that the business meets the highest standards of data privacy. It provides valuable information to users, supporting them to make their own assessments of data privacy risks.
Conclusion

Companies that want to demonstrate their compliance with GDPR — or a strategic commitment to data privacy — should give urgent consideration to data privacy assurance. Assurance or certification processes become more important now that GDPR has entered into force. Organizations that are not yet fully compliant need not wait before planning their privacy assurance needs. EY has extensive experience in the technical aspects of data privacy, and our professionals have deep knowledge of ISAE and SOC standards. We look forward to working with you.

Talk to us

EY uses a risk-based, multidisciplinary approach supported by robust tools and methodologies to help you manage risks around privacy, achieve timely and consistent GDPR compliance, and leverage the GDPR for wider strategic benefit.

To discuss how EY can help you use the GDPR as a catalyst for change, including those described in this brochure, please contact:

Tony De Bos  
EY EMEIA Financial Services Data Protection and Privacy Leader  
T: + 31 88 407 2079  
M: + 31 62 908 4182  
E: tony.de.bos@nl.ey.com

Dennis Houtekamer  
EMEIA Service Organization Control Reporting Leader  
T: + 31 88 407 8766  
M: + 31 62 125 2728  
E: dennis.houtekamer@nl.ey.com

Jatin Sehgal  
Partner, Ernst & Young LLP  
EY Global Leader of EY CertifyPoint  
T: + 31 88 407 3348  
M: + 31 62 908 4825  
E: jatin.sehgal@nl.ey.com
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.

© 2019 EYGM Limited.
All Rights Reserved.

EYG No. 03145-184GBL
EY-000085395.indd (UK) 04/19.
Artwork by Creative Services Group London.
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