Building a better working world

Demonstrating data privacy for GDPR and beyond

EY data privacy assurance services

Introduction

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

Organizations that want to demonstrate robust data 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.

Above all, Europe's GDPR enters force in May 2018. First proposed in 2012, the GDPR will apply uniformly across the EU and affect any organization operating in the EU. Its reach extends to support organizations, not just those collecting personal data.

The effects of the GDPR will be 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,[1] to help organizations comply with the GDPR.

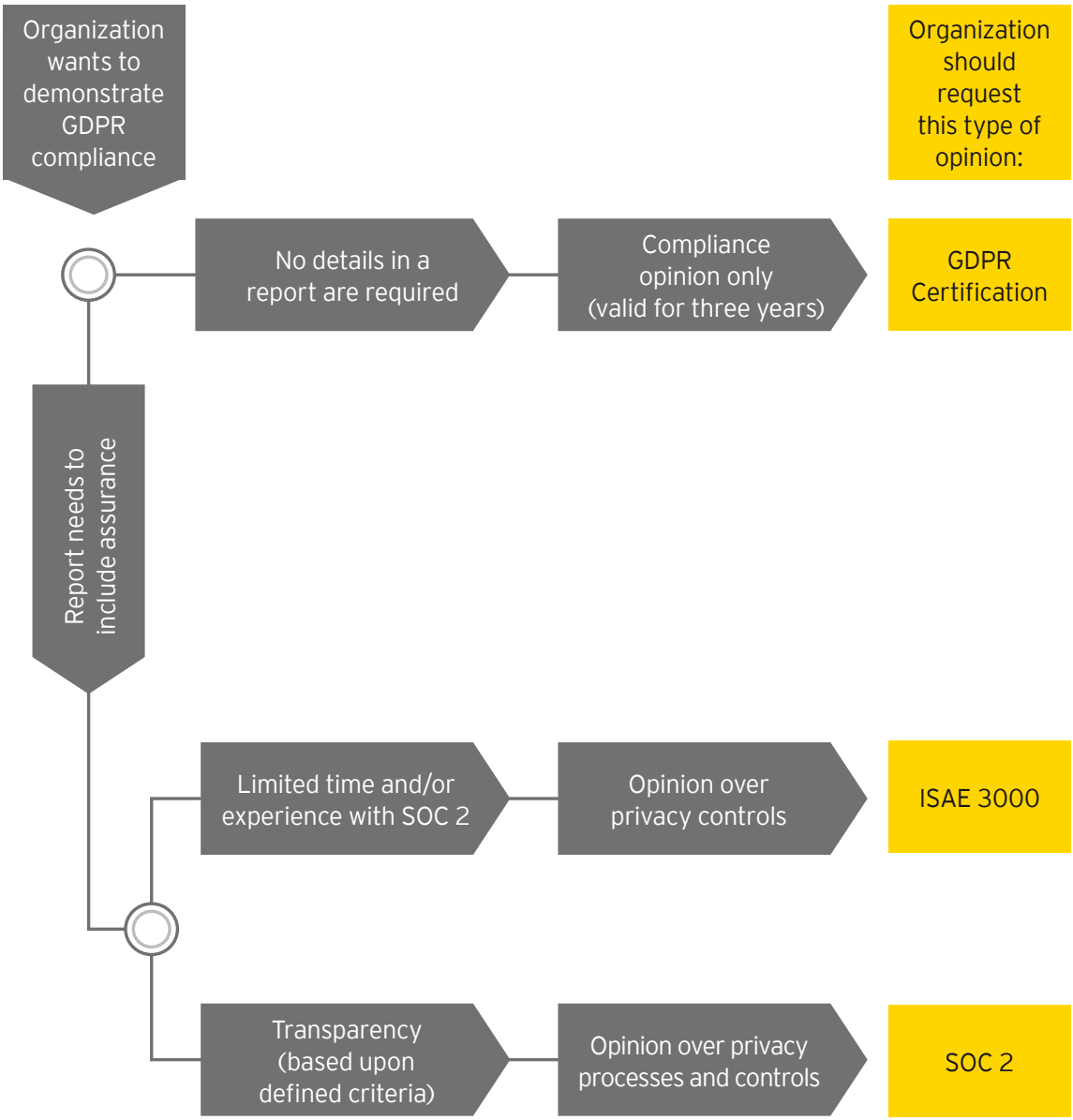
When it comes to demonstrating clients compliance with the GDPR, EY's data privacy assurance services give clients independent assistance about their data protection controls. The benefits of data privacy assurance include:

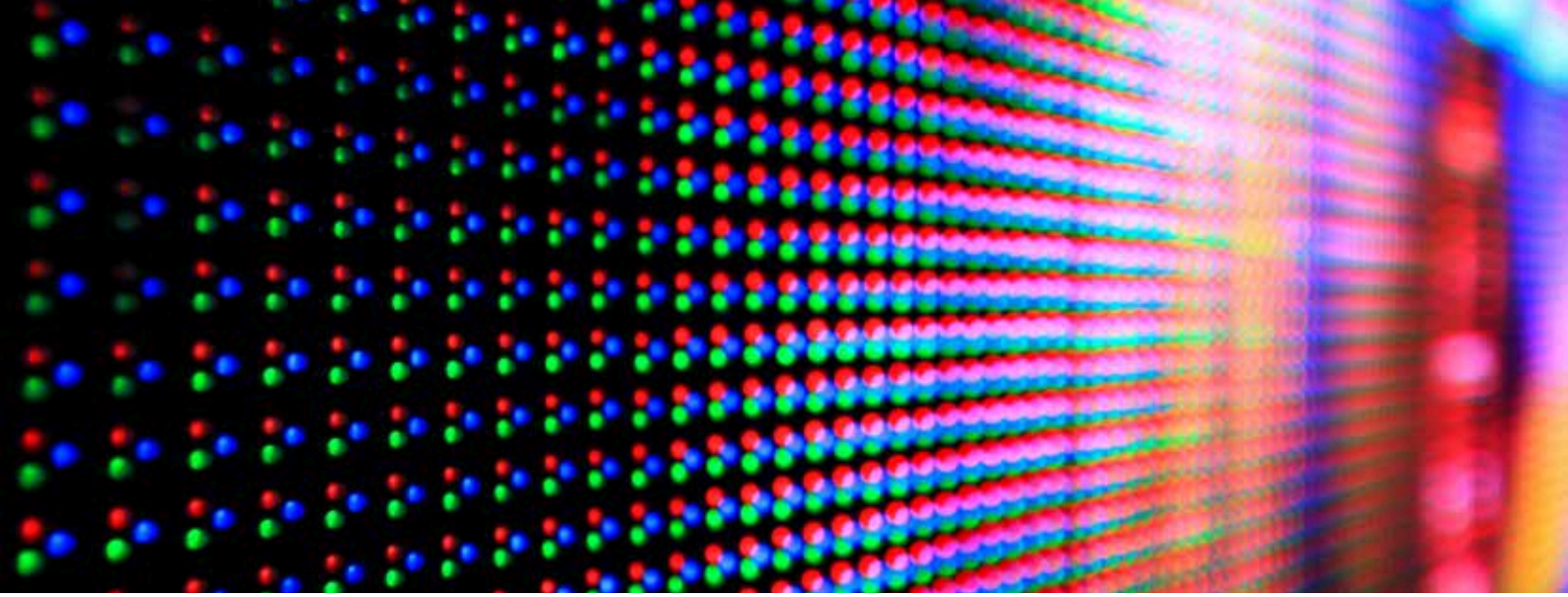
- Indicating compliance to supervisors and other external stakeholders
- Showing that organizations have implemented processes to protect personal data
- Demonstrating that organizations execute procedures to limit the possibility of a data breach

The three services that support achieving these benefits are 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).

[1] http://www.ey.com/Publication/vwLUAssets/ey-gdpr-what-you-need-to-know/$FILE/ey-gdpr-what-you-need-to-know.pdf

What does your organization need?





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 provide the business with GDPR Certification, which is a one-page statement stating the conformity to the requirements in the GDPR. It demonstrates that the business's privacy processes have been audited, but it does not include detailed disclosure. Certificates are valid for a period of time 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 be 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. The GDPR enters force in May 2018, so assurance or certification processes need to begin as soon as possible. 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

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.

EYG No. 03145-184GBL

EY-000058767.indd (UK) 05/18.
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.

ey.com