Building a better working world

When it comes to GDPR compliance, is 'OK for now' enough?

EY CertifyPoint's GDPR certification process will help you achieve and demonstrate compliance.

Minds made for protecting financial services

Introduction

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

Increasingly organizations need to demonstrate robust data protection to their stakeholders. To help provide this assurance many firms are looking to assessments and certification carried out by an impartial and independent professional body.

EY CertifyPoint, founded in 2002, is an accredited institute with experienced auditors all over the world. It offers an approach that can be tailored to the needs of every organization, which leads to GDPR certification. It has helped leading organizations become compliant with today's regulations.

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

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. Data protection laws worldwide are changing and becoming more demanding.

GDPR applies uniformly across the EU and affects organizations processing EU citizens' personal data. Its effects are far-reaching, and non-compliance may lead to fines of up to €20m or 4% of global revenues, whichever is the highest.

However, GDPR is only one driver of the privacy agenda. Consumer awareness of data privacy risks is 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 and not just as a compliance target. The ability to demonstrate robust data privacy has become a source of competitive advantage in many markets.

Other EY research explores this in detail and can be found at ey.com/fsgdpr.

Demonstrating compliance with GDPR certification

How we can help

Organizations that want to demonstrate their compliance with the GDPR first need to ensure that they meet its requirements.

The GDPR certification process provides an independent assessment of data protection controls specific to selected departments or processes within your organization. This could include personally identifiable information processing activity, carried out in the context of systems, products or services by an organization that may be a data controller or processor.

Certification is an approved mechanism under Article 42 of the regulation that encourages the use of data protection certification for the purpose of demonstrating compliance.

The benefits for a certified organization include, evidence that demonstrates compliance to supervisors, external stakeholders and customers, therefore increasing trust and providing competitive advantage. Certification will act as an investment, by generating return as companies accelerate their digital transformation, minimizing inaccuracy and improving risk management.

About our certification scheme

EY CertifyPoint's GDPR certification scheme involves a set of procedures and operational checks that EY CertifyPoint auditors perform within the scope of the certification and in line with the requirements of the regulation.

EY CertifyPoint is responsible for granting, maintaining, extending, restricting, postponing and withdrawing certifications for various ISO standards and other certification frameworks. We are the only certification body among the Big 4 professional services organizations who certify companies globally.

EY CertifyPoint is already an accredited certification body for ISO 17065:2012 which is a key requirement under the Article 43 of GDPR regulation. EY CertifyPoint has applied for its accreditation under the GDPR certification body program introduced by the Dutch Data Protection Authority Autoriteit Persoonsgegevens and the Dutch Accreditation Council Raad voor Accreditatie. EY CertifyPoint is able to issue GDPR certification for your organization in an un-accredited manner against our GDPR certification scheme aligned to the regulation and requirements of ISO 17065:2012 while our application for accreditation is being processed by national authorities.

The GDPR certification process

Following client application, an optional readiness check audit can be conducted to determine the organization's current state of compliance. If deemed ready, the initial audit will then take place.

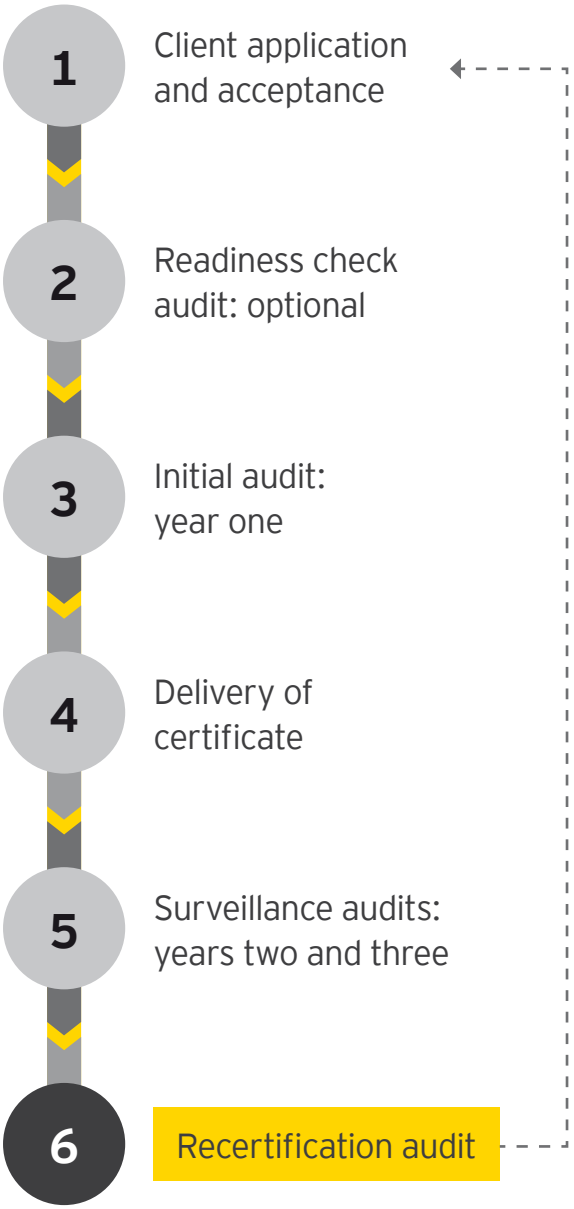
The audit process involves an experienced and certified team of auditors checking the compliance of the processing activities of the given organization against the GDPR certification scheme. The scheme includes relevant requirements of GDPR and is supported by our multi-disciplinary teams. The auditors use common auditing techniques, including documentation review, interviews and observations to assess whether the organization fulfils defined requirements.

The audit time depends on several factors including, the complexity and extent of the processing activities, the nature of the data being processed and whether the processing activities are based within or outside the EU, to name just a few.

Similar to the International Organization for Standardization (ISO) certification, an initial audit with a positive outcome results in a certificate, which is valid for three years. Surveillance audits will then be carried out in the following two years to confirm compliance is being maintained, and a recertification audit is performed before the certification expires.

Organizations can opt to audit one department, e.g., their sales or marketing department, and the specific processing activities of that department. Scope extensions are possible if they later decide to certify another department, or new significant processing activities are added to their services, e.g., a new product collecting different kinds of data using new privacy intrusive technologies. These scope extensions would require additional audit procedures to verify compliance with the certification is maintained.

Certification process



Conclusion

Companies that wish to demonstrate their compliance with GDPR – or a strategic commitment to data privacy – should give urgent consideration to GDPR certification. They need not achieve full compliance before planning their certification needs.

EY draws on extensive experience in the technical aspects of data privacy, and EY professionals have deep knowledge of certification standards. Through EY CertifyPoint, we can work with you from assessment through certification to ongoing audit, to help confirm compliance in this new era of data privacy.

Contacts

Jatin Sehgal
Partner and EY Global Leader,
EY CertifyPoint
Ernst & Young Accountants LLP

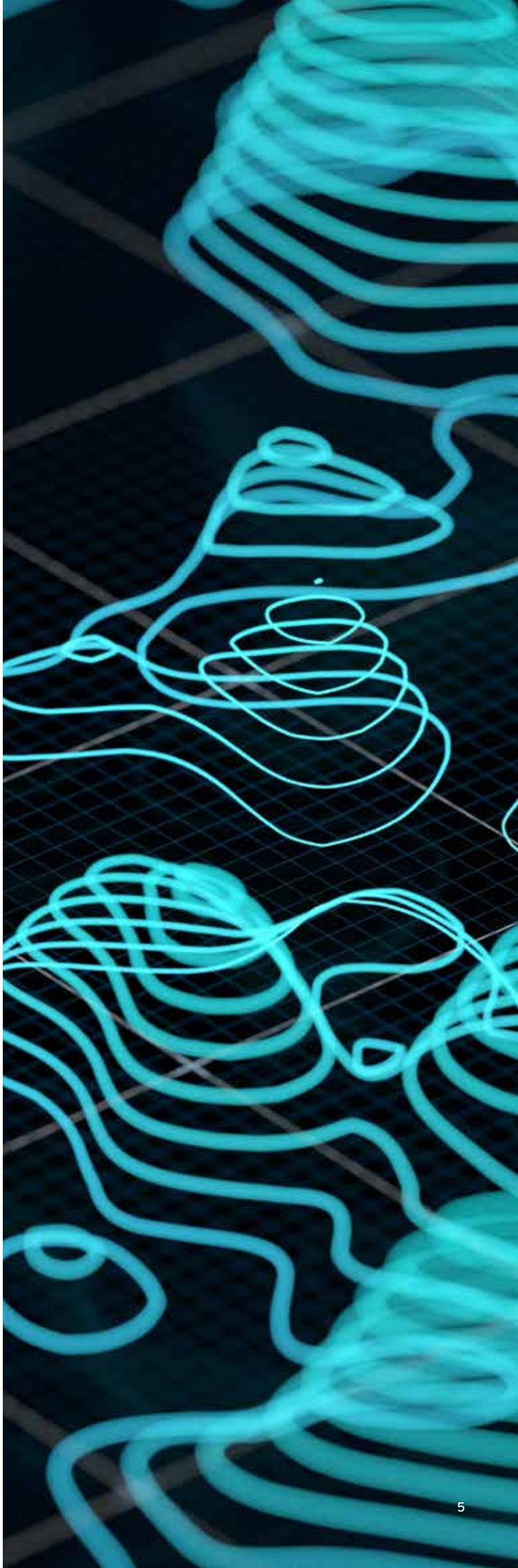
+316 2908 4825
jatin.sehgal@nl.ey.com

Tony de Bos
Partner and EY EMEIA Data Protection and Privacy Leader
Ernst & Young Accountants LLP

+316 2908 4182
tony.de.bos@nl.ey.com

Mayank Joshi
Manager, Security and Privacy Certifications
Ernst & Young Accountants LLP

+316 5544 2509
mayank.joshi@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.

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. 011291-18Gbl

EY-000071365.indd (UK) 10/18.
Artwork by Creative Services Group London.

ED None

ey.com/FSminds