



Are you prepared for the EU General Data Protection Regulation (GDPR)?

The European Union's new General Data Protection Regulation (GDPR) will come into force on 25 May 2018. GDPR requires organizations to put in place an appropriate governance framework when they collect and process personal information and empowers individuals to take control of their data. This means additional obligations that organizations need to comply with.

Non-compliance with the GDPR, even in the absence of any data breach, could be very expensive. Fines for non-compliance could reach €20 million or in case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding year, whichever is higher.

Companies should not wait for the GDPR to come into force. Instead, they should begin now to prepare their employees, processes and technologies to comply.

What is the scope of the GDPR?

The Regulation applies to any organization which processes personal data of individuals who reside in the European Union. Furthermore (and unlike the current Directive 95/46/EC), the Regulation also applies to organizations based outside the EU if they process personal data of EU residents.

What is 'Personal data' under GDPR?

As the European Commission explained when they initiated the GDPR, "personal data is any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address"¹.

What do Companies need to check?

Organizations will need to have a comprehensive understanding of the types of data they hold and their sensitivity within their IT environment; they will need to have information management policies, personal data registers/flows and internal data protection policies and processes in place.

Scope your personal data now - Organizations need to develop a comprehensive understanding of the scope of their environment, including the types of data held and their sensitivity. Likewise, they need to fully understand the flows of personal data within their company and identify any potential for breaches.

Look at what data you process - create an information management policy and data registers/flows - Knowing and having up to date data sources will help to ensure data confidentiality and assist information security practitioners in applying appropriate defense techniques. An information management policy is the roadmap for how data and information is captured in an organization. It should describe how data is collected, collated, captured and analyzed as well as define data flows and the roles of each person in the information management cycle.

¹ http://europa.eu/rapid/press-release_IP-12-46_en.pdf

Review your internal Data Protection policies and materials - Maintaining and enforcing internal data protection policies and procedures is a requirement under the GDPR. If policies and procedures do not exist, you will need to create these. If your organization already has policies and procedures in place, these will need to be reviewed in line with the new Data Protection regulations to ensure that the updated requirements are accounted for.

While some of the GDPR requirements are focused on organizational changes and priorities, others relate to Information Risk Management activities, where an internationally recognized standard, like ISO 27001, can help to implement the appropriate policies, procedures and controls.

How can Control Compliance Suite help you?

As stated in article 5 and article 32 of the GDPR, organizations should regularly assess and be able to demonstrate compliance with all the principles of the regulation.

In this context, Symantec Control Compliance Suite (CCS) will help you at two stages:

I. An initial Readiness Assessment

The Symantec CCS GDPR Readiness Assessment content will help organizations to evaluate their level of understanding of the Regulation, and estimate their current readiness on the path towards compliance with the GDPR. The overall outcome of this assessment will help organizations gauge how far they are from meeting certain important requirements of the GDPR. Based on the results of the assessment, action plans can be put in place. Note that this assessment can be launched multiple times to see the progression.

II. Compliance Automation

The ultimate goal of Symantec Control Compliance Suite is to help organizations implement a cost effective, holistic approach to procedural compliance automation, monitoring and tracking progress leveraging the CCS modules below:

- **Symantec CCS Policy Manager:** automates policy definition and policy life cycle management. Customers use Policy Manager to identify common controls across multiple mandates, update the content and technical standards updates on a regular basis, and manage the lifecycle of security policies, standards, and controls.
- **Symantec CCS Assessment Manager:** used to collect response to both readiness and full GDPR content questionnaires. Customers use these to assess the effectiveness of procedural security controls in the data center, to evaluate overall employee security awareness, and to support security awareness training.
- **Symantec CCS Standards Manager:** used to collect technical evidence of the data security enforcement. Organizations employ Standards Manager to discover and identify rogue and misconfigured assets, detect configuration drifts, and evaluate if systems are secured, configured, and patched according to the customer's security standards.

What to do next?

Work with one of our specialist partners to help you run your Control Compliance Suite GDPR Readiness Assessment and receive an executive action plan to help you prepare for compliance with the GDPR. Contact your Symantec sales account representative for more information.

More Information

Visit our website

<http://enterprise.symantec.com> or <http://go.symantec.com/ccs>

To speak with a Product Specialist in the U.S.

Call toll-free 1 (800) 745 6054

To speak with a Product Specialist outside the U.S.

For specific country offices and contact numbers, please visit our website.

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, is defining the future of cybersecurity by solving the industry's toughest challenges of securing mobile workforces, protecting the cloud, and stopping advanced threats. Organizations around the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Symantec operates the world's largest civilian cyber intelligence network, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

Symantec World Headquarters

350 Ellis St.

Mountain View, CA 94043 USA

+1 (650) 527 8000

1 (800) 721 3934

www.symantec.com