CohnReznick
ADVISORY • ASSURANCE • TAX

General Data Protection Regulation (GDPR): Are You On the Road to Compliance?

European Union (EU) General Data Protection Regulation (GDPR) — which went into effect on May 25, 2018 — is applicable to organizations that store, process, transmit, or use personal data collected from EU residents.

The risks of non-compliance may result in fines, class-action lawsuits, loss of customer trust, and a damaged reputation. Depending on the severity of the violation, fines may be as high as 20 million Euros or 4% of the previous year's global revenue. Organizations are also required to demonstrate continuous GDPR compliance and ongoing monitoring of their respective environments.

Whether your organization has operations in the EU or not, if your organization is collecting, storing, processing, using, or transmitting EU resident personal data, your organization must comply with the GDPR requirements. What follows is a high-level list of the major GDPR requirements (referred to as "articles") that most U.S.-based companies need to address:

- Data processing principles (Article 5)
- Legal basis for collecting sensitive data (Article 9)
- Controller's responsibilities (Article 24)
- Processor's responsibilities (Article 28)
- Cooperation with Supervisory Authority (Article 31)
- Data breach notification (Articles 33-34)
- Designate/support Data Protection Officer (DPO) (Articles 37-39)
- Sanctions and penalties (Articles 79-84)
- Legal basis for processing (Articles 6-8)
- Data subject (EU resident) rights (Articles 12-22)
- Privacy by design and default (Article 25)
- Record keeping (Article 30)
- Security safeguards (Article 32)
- Data Protection Impact Assessment (Article 35)
- Data transfers outside of European Economic Area (EEA) (Articles 44-49)
- Employment laws (Article 88)

Key Focus Areas

For organizations that have not started or are not fully GDPR compliant, take note of the key areas that should be in place or in process to show you are acting in good faith:

- Documentation of how your company processes personal data, why it is being processed, who else besides your organization processes the data and what data is being processed;
- A review and update of IT security, data privacy policies and incident response plan;
- A determination if you need to employ or outsource a Data Protection Officer (DPO);
- Employee education and awareness training on security and data privacy;
- Protocol for responding to requests from EU residents such as those who want their personal data to be removed from your company's systems;
- Data inventory and mapping of the information tracked when a customer goes to your website; and
- A notice on your website that gives customers the option to provide consent to receive any marketing information or tools (e.g. cookies).

CohnReznick

Advantages with CohnReznick

Our proven approach to helping organizations become GDPR compliant was developed by our cybersecurity and technology risk leadership team based on experience performing similar privacy engagements to support our global clients and the international privacy requirements of the various regions and countries. Our methodology is designed to holistically assess your organization's business processes and technology by using a combination of technical methods and techniques, to provide practical and feasible recommendations with a focus on the organization's ability to comply with the GDPR requirements.

Our step by step process ensures that all gaps against the GDPR requirements are identified and prioritized. We have years of experiences developing accelerated roadmaps to support our client's efforts to become GDPR compliant.

IDENTIFY

- Understand how and what type of personal data is collected
- Identify systems used to collect personal data
- Develop data flows and maps
- Review lawful collection of data
- Validate applicability of various GDPR articles and requirements

ASSESS

- Review and asses the data and system inventory
- Review current policies, procedures, and standards
- Review data transfers and vendor agreements
- Assess process involved in satisfying GDPR requirements
- Conduct a system readiness assessment for privacy and data protection requirements
- Conduct a privacy and impact assessment
- Assess security incident and breach notification plans

REMEDIATE

- Update policies, procedures, and standards
- Update/enhance privacy plans
- Update/enhance security incident and breach notification plans
- Implement Data Protection Impact Assessment (DPIA) strategies
- Validate applicability of various GDPR articles and requirements
- Develop an ongoing GDPR compliance plan

MONITOR

- Conduct annual privacy and data protection audits
- Assist with monitoring compliance with GDPR requirements

About CohnReznick's Technology Risk and Cybersecurity Practice

CohnReznick has been providing cybersecurity and technology risk services for more than 15 years, and our experience in this area has provided us with a strong foundation to help organizations balance a wide array of technology and cybersecurity-related risks to help protect their brands and assets.

Our technology risk and cybersecurity practice comprises experts in the assessment of strategic cybersecurity risk, evaluation, design, and remediation of IT security strategy and controls. The experience of the group is extensive, having delivered these services on numerous engagements. We utilize a methodology that is focused on identifying impactful risks and making solid recommendations to improve an organization's IT security posture and control. Our automation and technology tools are leading edge, which enables us to maintain a highly effective work plan.

For further information on GDPR, please contact:

Shahryar Shaghaghi
Cybersecurity and Privacy leader
CohnReznick Advisory
646-601-7899 | Shahryar.Shaghaghi@cohnreznick.com

Bhavesh Vadhani, CISA, CRISC, CGEIT, PMP
Principal
CohnReznick Advisory
703-847-4418 | bhavesh.vadhani@cohnreznick.com

About CohnReznick

CohnReznick LLP is one of the top accounting, tax, and advisory firms in the United States, combining the deep resources of a national firm with the hands-on, agile approach that today's dynamic business environment demands. With diverse industry expertise, the Firm provides companies with the insight and experience to help them break through and seize growth opportunities. The Firm, with origins dating back to 1919, is headquartered in New York, NY with 2,700 employees in offices nationwide. CohnReznick is a member of Nexia International, a global network of independent accountancy, tax, and business advisors.

For more information, visit **www.cohnreznick.com**.