



INSIGHTS: Risk and Business Advisory

GDPR Compliance Deadline Is Rapidly Approaching

European Union (EU) General Data Protection Regulation (GDPR) is applicable to organizations that store, process, transmit, or use personal data that they collected from EU residents. Any organizations that need to adhere to the GDPR regulation must start implementing a plan to be compliant before the rapidly-approaching deadline of May 25, 2018.

The risks of ignoring this deadline 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. The GDPR also requires organizations to be able to demonstrate continuous compliance and ongoing monitoring of their respective environments.

Per a recent survey conducted by both tech-compliance and security company TrustARC, and the International Association of Privacy Professionals (IAPP)*, it was noted that 67% of the organizations surveyed indicated that they will not be compliant with GDPR before May 25. Only 40% of U.S. firms revealed that they have just started their implementation plan to be compliant.

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 will need to comply with the GDPR requirements. What follows is a high-level list of the major requirements (referred to as "articles") that most U.S.-based companies will need to address to become GDPR compliant:

- 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 Items to Accomplish Before the Deadline

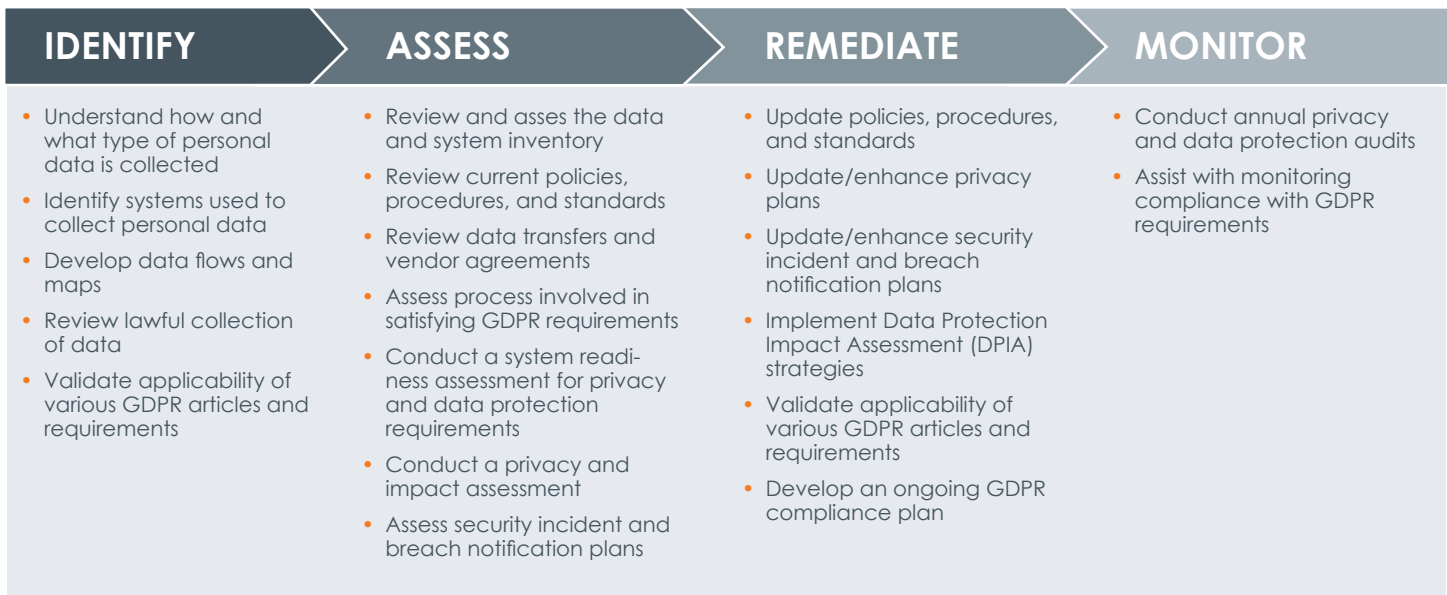
For organizations that have not started or know that the GDPR compliance deadline will not be met, take note of the key activities you should start implementing before the deadline:

- Document 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;
- Review and update relevant IT security, data privacy policies and your incident response plan;
- Determine if you need to employ or contract with a Data Protection Officer (DPO);
- Provide education and awareness training to the staff around security and data privacy;
- Determine how you will respond to requests from EU residents such as those who want their personal data to be removed from your company's systems;
- Determine what information is tracked when a customer goes to your website; and
- Are you ensuring that your website provides a way for its customers to consent to receive any marketing information or tools (e.g. cookies)?

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 other techniques, and 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.



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 is comprised of 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

Bhaves Vadhani, CISA, CRISC, CGEIT, PMP

Principal
CohnReznick Advisory
703-847-4418 | bhaves.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.

© 2018 CohnReznick LLP

This has been prepared for information purposes and general guidance only and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is made as to the accuracy or completeness of the information contained in this publication, and CohnReznick LLP, its members, employees and agents accept no liability, and disclaim all responsibility, for the consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.