




EU GENERAL DATA PROTECTION REGULATION STEPS TO TAKE RIGHT NOW

The biggest change to European data protection legislation in twenty years is looming. The GDPR, which overhauls and harmonizes data protection law in Europe, will come fully into effect in May 2018, and all companies that offer goods and services to individuals in the EEA must comply with the new law. Many U.S.-based companies are realizing that the GDPR applies to them too – even if they don’t have offices in Europe! It is critical for companies to act now, since the new law introduces significant anti-trust-like fines (4% of annual worldwide turnover or 20 million euros, whichever is higher) for noncompliance.

WHAT TO DO

	<p>Generate Awareness</p>	<ul style="list-style-type: none"> ▶ Ensure that key decision makers in your company are aware that the law is changing and that the impact to your organization is potentially substantial. ▶ Secure a budget to ensure you will have the resources needed to build and implement a compliance plan.
	<p>Conduct a Gap Analysis Against Core GDPR Requirements</p>	<ul style="list-style-type: none"> ▶ Data flow analysis – determine what personal data is held in your organization, where it came from, and whom you share it with. ▶ Review of data collection – determine whether the personal data collected is limited to the information necessary and relevant to the purpose for which it was collected. ▶ Review privacy policies to determine whether adequate information is provided, such as your identity, the type of data you intend to collect, and how you intend to use the data. ▶ Review policies/procedures for maintaining data quality. ▶ Review documentation processes – demonstrating compliance is key under the GDPR. ▶ Review the legal basis for processing personal data (e.g., consent, legitimate interest, etc.). ▶ Review the legal basis for transferring data outside the EEA (e.g., BCRs, Privacy Shield Frameworks, standard contractual clauses, etc.) ▶ Review the readiness of your security programs, including whether the organization is prepared for a data breach. ▶ Review privacy program management – Is a process in place to train employees on privacy? Are controls in place to ensure that PIAs are being conducted? Consider whether you need to appoint a data protection officer.
	<p>Compliance Roadmap</p>	<ul style="list-style-type: none"> ▶ Develop a compliance road map based on any gaps identified – put together a team, designate roles and responsibilities, and set project milestones.

CONTACT:

Shannon K. Yavorsky
skyavorsky@Venable.com
+1 415.343.4486

Kelly DeMarchis Bastide
kabastide@Venable.com
+1 202.344.4722

Emilio W. Civitanes
ewcivitanes@Venable.com
+1 202.344.4414