SEYFARTH SHAW

A Perfect Privacy Storm

Are you ready for the EU GDPR?

The EU-U.S. Privacy Shield is the calm before the storm of the EU General Data Protection Act (GDPR) arriving May 2018. GDPR will impact all U.S. companies doing business in the EU. Here is what GDPR will mean for your business.

Why does the EU GDPR Matter?

- Significant Financial Penalties for Violations
- Broad Enforcement and Audit Authority by EU Data Privacy Officials
- Substantial Time and Cost for Implementation of GDPR Privacy Design Principles, the Right to Be Forgotten, and the Right to Portability
- Significant Time and Cost to Comply with the 72-hour Data Breach Notice Requirement

Seyfarth's eDiscovery and Information Governance (eDIG) Practice Group and Global Privacy and Security (GPS) Team have developed risk assessment tools and remediation strategies, and leverage their data privacy, data security, complex litigation and global employment law expertise to reduce the cost of EU GDPR compliance.

For more information, contact your Seyfarth attorney, or a member of eDIG Practice Group or GPS Team.

GDPR imposes fines of up to 4% of global revenue or up to 20 million Euros whichever is greater.

Only a small number of U.S. companies are aware of, and far fewer are prepared for GDPR.

GDPR is ambiguous as to whether cross-border pretrial discovery will be allowed for U.S. cases.

GDPR has been characterized as a seismic shift for global data privacy and protection.

GDPR By The Numbers

508M	508 million people live in the EU
38%	Only 38% of U.S. companies are aware of specific EU GDPR requirements
28%	The EU represents 28% of global GNP
03%	Only 3% have a plan for EU GDPR.
02%	Only 2% of Cloud Applications are EU GDPR-ready

Specific EU GDPR Requirements

1. Companies must (1) have a legal basis for processing data; and (2) mandate processor GDPR compliance by contract. This will make processors directly liable for the security of EU personal data.
2. The international transfer (and onward transfer) of EU personal data to the United States for business and legal matters will be governed by the GDPR. The GDPR will preempt Privacy Shield to the extent of any differences.
3. Obtaining consent for the processing of EU personal data must be clear, and include an "opt-in" process; and for children under the age of 16, express parental/guardian consent is required.
4. Companies that process large volumes of personal data must appoint a Data Protection Officer (DPO), which will be and considered best practice for all.
5. Company IT systems that handle any EU personal data must, by default, apply "Privacy-by-Design" controls.
6. Privacy Risk Impact Assessments will be required for projects that involve a high degree of privacy risk, particularly those involving sensitive EU personal data.
7. International companies will now, in principle, have a "one-stop-shop," and will only have to deal with one Data Protection Authority.
8. GDPR will broaden the definition of types of personal data to include identifiers such a genetic, mental, economic and social information, among others.

GDPR Compliance Checklist

- ☑ Are your "C" Suite Executives aware of the time and cost of GDPR compliance and consequences of non-compliance?
- ☑ Can you identify (1) what kind of EU personal data is handled by your company; and (2) where the personal data is located—including IT systems that create, process, store, and transmit EU personal data; and (3) do such IT systems, by default, comply with GDPR Privacy by Design requirements?
- ☑ Do you have a data breach response team and plan to enable your company, as required, to (1) notify the EU Data Protection Authorities (DPAs), within 72 hours of a breach; and (2) notify the affected individuals "without undue delay"?
- ☑ If you process large volumes of personal data, or certain special categories of personal data, have you taken steps to appoint and develop a governance plan for your company Data Protection Officer (DPO)?
- ☑ Have you (1) modified existing contracts with processors to be GDPR-compliant; and (2) developed a protocol and mechanism(s) for (a) transfers of EU personal data to the U.S. for business purposes; and (b) cross-border transfers of EU personal data (including onward transfers) for U.S. discovery in litigation or regulatory proceedings?
- ☑ Do you have a means of implementing (1) the Right to Be Forgotten, involving erasure of EU personal data, upon proper request; and (2) the Right to Data Portability, involving delivery of individual EU personal data in a portable, easily usable format?

Seyfarth's eDiscovery & Information Governance Practice Group and GPS Team provide practical and innovative legal advice and solutions for information governance, including data privacy and security. More information can be found at our Carpe Datum Law Blog (**www.carpedatumlaw.com**).

SEYFARTH SHAW