PERKINSCOIE

Privacy & Security

GENERAL DATA PROTECTION REGULATION (GDPR)

THE GENERAL DATA PROTECTION REGULATION (Regulation (EU) 2016/679) replaces the EU Data Protection Directive (Directive 95/46/EC) as the framework for EU privacy and data protection. The GDPR goes into effect on May 25, 2018, and for most companies doing business in the EU, coming into compliance will require significant time and resources.

WHAT YOU NEED TO KNOW ABOUT THE GDPR

EXPANDED SCOPE: **Companies that do not have any physical presence in the EU may be subject to the GDPR.** The extraterritorial reach of the GDPR is much broader than the Directive's, and it applies to entities that have an establishment in the EU, offer goods and services to EU data subjects, or monitor the behavior of EU data subjects. In addition, the GDPR expands the definition of "personal data" to include, among other things, online identifiers, device identifiers, cookie IDs and IP addresses.

ENHANCED RIGHTS FOR DATA SUBJECTS: **Under the GDPR, companies will be required to provide individuals with greater visibility into and control over how their personal data is processed.** The GDPR provides explicit requirements for the type of notice companies must provide before processing the personal data of an EU data subject. It also grants data subjects broad rights regarding the treatment of their personal data, including the right to be forgotten, the right to access and correct data, the right to data portability, the right to restrict certain processing and the right to object to automated decision making. Companies need to review, and likely revamp, their data practices and procedures to ensure that they can meet these obligations.

PRIVACY BY DESIGN AND BY DEFAULT: **Companies subject to the GDPR will be required to institutionalize privacy.** Privacy by default requires companies to limit collection, processing and storage of personal data. Privacy by design requires companies to implement appropriate technical and organizational measures when determining the means of processing data and when processing data. For example, whenever possible, companies are encouraged to implement pseudonymization by processing personal data in
a manner such that it can no longer be attributed to a specific data subject. Additionally, the GDPR outlines standards regarding the security of data processing for both data controllers and data processors. Where a type of processing uses new technology or is likely to result in a high risk to data subjects, including profiling or large-scale processing of special categories of data, the data controller is required to carry out a privacy impact assessment. This assessment must be detailed and documented, and where the assessment indicates a "high risk," prior consultation with a supervisory authority is required.

ACCOUNTABILITY: **The way companies ensure and demonstrate compliance with the GDPR will be scrutinized.** The GDPR requires companies to keep clear and accurate records of their data processing activities and compliance efforts. Companies must document the flow of data within their organization and provide detailed information in the event of an audit. Companies may be required to designate a data protection officer to advise and monitor their compliance and to determine whether a data protection impact assessment is required. The GDPR also imposes a high duty of care on data controllers in selecting service providers to process personal data on their behalf. Data processing contracts must be implemented and must include a range of specific information and obligations. Service providers have similar obligations to pass these contractual requirements down to any sub-processors.

BREACH NOTIFICATION: **The GDPR introduces a new security breach notice requirement.** In the event of a breach, companies must provide prompt, detailed notification to the supervisory authority and, if a breach "is likely to result in a high risk to the rights and freedoms of individuals," to the affected data subjects.

PENALTIES: **Failure to comply with the GDPR can result in substantial potential liability, including steep penalties imposed by regulators, which can extend to a company's vendors and service providers.** Penalties vary depending on the type of violation, but can be as high as 20 million euros or 4% of a company's worldwide annual turnover. Additionally, the GDPR grants individuals permission to sue if harmed by a company's violations.

HOW WE CAN HELP

If you have not already started, now is the time to begin the process of reviewing your company's compliance with the GDPR. Perkins Coie's Privacy & Data Security lawyers have a deep understanding of the GDPR requirements for both data controllers and data processors, and regularly counsel companies doing business in the EU to help them meet the GDPR's requirements. Our clients rely on us to help them:

- Fully understand their current privacy and data protection procedures;
- Revise existing practices, procedures and governance frameworks to comply with the GDPR;
- Analyze where current procedures fall short of the GDPR requirements; and
- Design and implement new privacy and data security policies, procedures and governance frameworks.

Over the last decade we have acted as the global strategic quarterback for many clients, helping them develop comprehensive privacy and data security programs that protect them from legal exposure in countries around the world.

WHAT OTHERS SAY

- Ranked Tier 1 nationally for Information Technology Law by *U.S. News—Best Lawyers*®, 2016
- Named "Law Firm of the Year" for Technology Law by *U.S. News—Best Lawyers*®, 2015
- Ranked nationally in Privacy and Data Security Law and in key markets by *Chambers USA*, 2017
- Named as one of the top law firm "Litigation Powerhouses" by *Law360*, 2016
- Named a "Leader" among tech-savvy law firms based on corporate counsel feedback to *BTI Brand Elite*, 2016
- Ranked in Tier 1 for International Trade & Transactions Law by *U.S. News—Best Lawyers*®, 2016

THOUGHT LEADERSHIP

We help our clients stay abreast of regulatory changes and recommend specific responses to these changes. We produce and distribute updates, articles and presentations on emerging issues and other topics of note to our clients. Select materials are linked below:

- Europe's New Global Data Protection Law
- Summary of Significant Changes to the GDPR

Commented [NN1]: This needs to link to the right doc. Let's discuss.