CRAVATH, SWAINE & MOORE LLP

David J. Kappos
+1-212-474-1168
dkappos@cravath.com

Rachel G. Skaistis
+1-212-474-1934
rskaistis@cravath.com

SLAUGHTER AND MAY

Rob Sumroy
+44-20-7090-4032
rob.sumroy@slaughterandmay.com

Rebecca Cousin
+44-20-7090-3049
rebecca.cousin@slaughterandmay.com

GDPR

May 16, 2018

On May 25, 2018, the General Data Protection Regulation (GDPR), the European Union's comprehensive data privacy and protection regime, will come into effect. The GDPR replaces the E.U.'s prior directive governing the processing and transfer of personal data, which has been in place since 1995. Sweeping in both its jurisdictional reach and scope, the GDPR seeks to cover "any information concerning an identified or identifiable natural person" and in certain cases has extra-territorial effect.

The regulation imposes new obligations on "controllers" and "processors" of protected personal data and contemplates significant penalties when covered entities fail to satisfy their obligations (fines may be as large as the higher of €20,000,000 or 4% of annual worldwide turnover). The GDPR generally holds controllers–companies that set the "purposes and means" for processing–responsible for ensuring compliance with its requirements, including implementing various technical and organizational measures, maintaining certain records and notifying appropriate parties of data breaches. Data processors–companies that conduct processing on the controller's behalf–are responsible for, among other things, taking measures to ensure the security of processing, limiting the scope of processing to the controller's instructions and assisting the controller in ensuring GDPR compliance.

The GDPR applies to all controllers and processors who either (A) maintain an "establishment" in the E.U., broadly speaking being a stable physical presence whatever the size, in which case the GDPR covers the processing of personal data "in the context of" that E.U. establishment, regardless of where the processing takes place, or (B) offer goods or services to individuals in the E.U., in which case the GDPR covers the processing of data related to such offering, or (C) monitor the behaviour of individuals in the E.U., in which case the GDPR covers the processing of data related to such monitoring. Controllers or processors who are not established in the E.U. must appoint a representative in the E.U.

If the GDPR does apply to your business, some of the key implications may include:

- individuals must be made aware of what personal data you hold and what you do with it
- processing of data must be "fair," and must meet one of the listed grounds permitting processing
- processing of data must occur only as compatible with your legitimate objectives, and only with respect to data necessary for those objectives
- controllers must adopt a "data protection by design" approach to ensure that privacy implications are considered before proceeding with, as well as during, any processing

- processing of data by a processor must be governed by a contract or other legal act, which must include a list of stipulated provisions aimed at protecting individuals
- processing of data must ensure appropriate security of the data
- controllers must notify relevant data protection authorities (within 72 hours) and potentially affected individuals in the case of a data breach if certain thresholds are met
- individuals have certain rights regarding their personal data, including the right to access, correct and erase.

Clients may have already taken steps to assess whether they are covered by the new regulation and to bring themselves into compliance. With the effective date rapidly approaching, we write to remind clients of the GDPR's broad coverage and to suggest discussing any concerns with counsel as soon as possible.

Global organizations handling personal data can be faced with complex and challenging regulatory regimes to contend with as data flows across borders. Both our firms take a pragmatic and commercial approach in guiding our clients through the regulatory maze, avoiding the pitfall of viewing data protection compliance and privacy merely as a legal 'box-ticking' exercise. We understand that good privacy practices need not be inconsistent with successful business, and in fact can offer a strong foundation for positive customer engagement.

Should you have questions, please do not hesitate to contact us at Cravath or Slaughter and May.