ROPES & GRAY

ROADMAP TO COMPLIANCE

EU GENERAL DATA PROTECTION REGULATION

PLAN NOW FOR GDPR COMPLIANCE

The European Union's General Data Protection Regulation (GDPR), which seeks to unify fragmented existing data protection rules, will become fully enforceable throughout the EU (including the United Kingdom) on May 25, 2018. It imposes significant new obligations on organizations that control or process relevant personal data, and failure to comply may have major financial consequences. With so much at stake, data controllers and processors will want to take immediate action to prepare for enforcement of the GDPR.

HOW WE CAN HELP

Ropes & Gray is committed to helping you determine how the GDPR applies to your organization and working with you to adapt your policies and procedures to ensure compliance. That's why we developed the *Roadmap to Compliance*, a workbook that walks in-house teams through practical steps they can take to address GDPR requirements and demonstrate compliance by May 25, 2018. It includes:

- A summary of relevant GDPR requirements, organized by topic
- A practical explanation of what these requirements mean for businesses
- A checklist of proposed action items that will position an organization for GDPR compliance

WHY ROPES & GRAY

Ropes & Gray advises on all aspects of privacy and cybersecurity law, including undertaking comprehensive privacy and security assessments, building global compliance programs for businesses operating across multiple jurisdictions and industries, negotiating contracts concerning vendor relationships, and assessing and addressing the privacy and security risks in corporate transactions.

Drawing on this extensive experience, our privacy & cybersecurity group is ready to help organizations in a wide range of business sectors—including financial services, asset management, technology, retail, consumer products, health care and life sciences, manufacturing, food and beverage, media, academic institutions, and energy—understand the key implications of the GDPR and develop a compliance plan. We have an established team focused on assessing GDPR developments for our clients worldwide, including any changes that affect compliance.

Our privacy & cybersecurity team is composed of attorneys in the firm's offices in Asia, Europe and the United States, allowing us to provide real-time advice worldwide. In jurisdictions in which we do not have an office, we work seamlessly with our network of data protection experts to address local laws, cultural nuances and geographical considerations. This network allows us to deliver efficient, cost-effective advice on every continent, streamlining multinational reviews and reducing administrative burdens. We drive positive privacy and security change across our clients' platforms—wherever our clients do business. ▶

***ROADMAP TO COMPLIANCE*, A STEP-BY-STEP GUIDE TO GDPR COMPLIANCE**

DEVELOPING YOUR COMPLIANCE ROADMAP

To lay the groundwork for your organization's GDPR compliance program, Ropes & Gray first evaluates your current compliance structure and procedures. After concluding this assessment, our team will partner with you on each step of your compliance roadmap. These steps include:

- **DEVELOPING A GOVERNANCE STRUCTURE.** We will work with you to design a responsibility structure that fits your organization, determining whether to appoint a data protection officer, and, for organizations not established in the EU, appointing a representative in the EU who can act on your organization's behalf on all issues relating to processing.

- **UPDATING INTERNALLY FACING POLICIES AND PROCEDURES.** We will work with you to implement data protection by design and default, satisfy new and more stringent requirements regarding consent and recordkeeping, and conduct data protection impact assessments when your organization leverages and uses data in a manner likely to create a substantial risk to the rights and freedoms of individuals.

- **IMPLEMENTING MECHANISMS TO ACCOMMODATE DATA SUBJECT RIGHTS.** The law requires that data controllers provide information notices to individuals regarding their personal data and after certain data breaches. Controllers must also respond to requests relating to individuals' rights under the GDPR. Ropes & Gray will work with you to develop the new processes necessary to accommodate requests and identify data.

- **CLOSELY MANAGING VENDORS.** Data controllers will want to perform due diligence of vendors with access to EU personal data to ensure that these vendors also comply with the GDPR. Our team can review existing contracts to make certain that vendors meet specific GDPR requirements; we can also develop a standard form addendum for new vendor agreements and advise you on how to add these new clauses to current contracts without renegotiating existing provisions.

- **RESTRICTING INTERNATIONAL DATA TRANSFERS.** Transfers of personal data to a third country or international organization outside the EU can only occur if the safeguards set forth by the GDPR are in place. While this mandate also applied under the Directive, the list of acceptable safeguards has changed, and since this area of the law is still evolving, Ropes & Gray can help data controllers and processors evaluate any existing mechanisms to ensure that they continue to serve their intended purpose.

- **IMPLEMENTING APPROPRIATE DATA SECURITY AND INCIDENT RESPONSE MEASURES.** Data controllers and processors are required to implement technical and organizational security measures to protect personal data; the GDPR also imposes an obligation on data controllers to disclose the occurrence of certain personal data breaches to the supervisory authority within 72 hours. The Ropes & Gray team can work with your organization to make sure that you have appropriate security measures in place and are fully prepared to respond in the event of an incident.

- **ABIDING BY SEALS, CERTIFICATIONS AND CODES OF CONDUCT.** The GDPR strongly encourages approved codes of conduct and certifications for the purposes of guiding data controllers and processors on GDPR requirements. Ropes & Gray can help you develop certifications and codes appropriate for your organization.

- **ESTABLISHING AN ONGOING MONITORING PROGRAM.** If desired, Ropes & Gray can work with your organization to establish a mechanism for tracking regulatory developments and guidance, interpretative decisions, and local requirements relating to the many areas of the GDPR reserved to Member States. Remember: May 25, 2018 marks only the beginning of the GDPR, which is certain to evolve to meet new needs and challenges.

CONTACTS

Heather Egan Sussman
Partner, Boston
heather.sussman@ropesgray.com
+1 617 951 7125

Rohan Massey
Partner, London
rohan.massey@ropesgray.com
+44 20 3201 1636