General Data Protection Regulation

The General Data Protection Regulation (GDPR) changes the European privacy law landscape significantly. GDPR creates one privacy rule for anyone who handles information about European residents or individuals located in Europe (Data Subjects) and replaces the previous EU directive. It sets more stringent reporting and documentation requirements, gives Data Subjects more control over their personal information, includes rules for reporting data breaches, has extra territorial effects, and for the first time, imposes high financial penalties for noncompliance.

Loeb is widely recognized for excellence in advising on the many U.S. and international privacy regulatory issues companies face as they collect, use, and store data and information. We have represented companies of all sizes and from a wide range of industries, including advertising, media, communications, technology, life sciences, consumer products and others. We regularly work with clients to develop data security protocols, processes and procedures compliant with the ever-changing privacy legal landscape. Our U.S. and EU privacy practitioners are closely monitoring the GDPR and are well-positioned to help clients in the U.S. and abroad proactively address GDPR compliance.

What Does the GDPR Do?

- Creates a single privacy rule for all of Europe
- Replaces the current EU Directive 95/46/EC
- Regulates **processing** of **personal data**
- Ensures Data Subjects have control over their data
- Requires accountability

How Does It Change European Law?

- Requires extensive documentation of data processing and privacy protection
- May require companies to appoint a Data Protection Officer (DPO)
- New data breach reporting obligations
- New requirements for vendor contracts
- Stringent penalties for noncompliance—up to 4% of annual revenue

Who Does It Impact?

- Companies located anywhere that process personal data of Data Subjects
- Data controllers (who direct data processing)
- Data processors (who perform operations)
- Companies seeking to do business with other companies that have European operations

Key Definitions

"Processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Personal data" means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

PREPARATION FOR GDPR COMPLIANCE

Identify DPO, if needed

- DPO needs substantive industry knowledge, privacy expertise
- DPO should be independent, have high-level access (boards and top executives)

Preliminary assessment

- Survey or interview key personnel throughout company
- Review data flows and processes
- Review contracts and written policies

Investigate data collection

- Source of data
- Permissions or consent obtained

Investigate data processing

- What purposes is data used for?
- How is data handled and protected?
- Is data combined with other data sets?
- Is data stored or archived?
- Is data transferred across borders? Outside of Europe?

Investigate data sharing

- Who has access to the data within the company?
- What vendors or subcontractors assist with processing?
- Who receives reports or results?
- Which third parties get access to data?
- Can third parties use for their own purpose?

Determine legal basis for processing

- Consent
- Contracts
- Employment relationship
- Legal obligations
- Company's legitimate interests
- Research/public good

Assess vendors and contracts

- Processors must also comply with GDPR
- Controllers must review protections and receive assurances
- Contracts must include adequate terms and assurances

Document data processing and legal justification

- Data Mapping
- Data Protection Impact Assessments (DPIAs)

Mitigate risky processes

- Adequate security
- Access controls
- Pseudonymization or de-identification
- Data minimization

Develop and document policies and procedures

- Create data governance process to ensure privacy by design and default
- Create processes to provide, correct or delete data when Data Subjects ask

Review security/protocols, create incident response plan

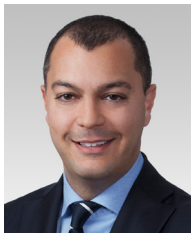
- Work with security team to develop plan and ensure implementation
- Put procedures in place to report breaches to regulators

Train employees

- Regulators require key employees to be trained on privacy regulations
- Training reduces risk of mishandling; ensures respect for privacy

OUR GDPR TEAM LEADERS

James D. Taylor
Co-Chair, Advanced Media and Technology
212.407.4895
jtaylor@loeb.com



Ieuan Jolly
Partner
212.407.4810
ijolly@loeb.com

Jessica B. Lee
Partner
212.407.4073
jblee@loeb.com

Susan E. Israel
Of Counsel
212.407.4177
sisrael@loeb.com