CYBERSECURITY AND PRIVACY

GENERAL DATA PROTECTION REGULATION

FACT SHEET

HONIGMAN®

General Data Protection Regulation Fact Sheet

On 27 April 2016, the European Commission adopted the General Data Protection Regulation (GDPR), a comprehensive replacement of the EU Data Protection Directive. The intention of the new regulation is to harmonize data protection laws across the EU and make it easier for companies to comply with the laws in multiple jurisdictions.

1. What is GDPR?

GDPR is a comprehensive overhaul of EU data protection laws. The new regulation replaces the previous regulatory regime and adds several new compliance requirements for companies handling personal data of EU citizens. Specifically, GDPR strengthens the rights of the individual whose personal data is obtained, allowing the individual to exert greater control over his or her data. Also, companies must adhere to higher standards for managing EU personal data and report data breaches.

2. Who must comply with GDPR?

In short, any company that collects, stores, handles, or uses EU personal data must comply with GDPR. More specifically, the new regulation applies to all "controllers" and "processors" of EU personal data:

- Data Controller: Entity determining how and why personal data is processed
- Data Processor: Entity processing personal data as directed by the data controller

3. What information is subject to GDPR?

The definition of "personal data" under GDPR is largely similar to the EU Data Protection Directive: information related to an identified or identifiable individual. However, GDPR does expand the definition of "personal data" to now include unique identifiers (e.g., IP addresses) and location data. Also included in the expanded definition is "pseudonymous data," or data that has been subjected to technological measures so that it can no longer identify an individual without using additional information.

Lastly, GDPR specifies new types of "sensitive personal information" that must be protected under the regulation, including genetic and biometric data.

4. When must companies be in full compliance with GDPR?

GDPR has technically been in effect since May 2016, but companies have a grace period until 25 May 2018 to reach full compliance with the new requirements.

5. What are the consequences for non-compliance with GDPR?

Companies that fail to comply with GDPR run the risk of regulatory investigations, as well as fines up to 4% of annual revenue. Although GDPR specifies penalties for certain types of offenses, the regulation also makes it clear that data protection authorities in individual EU member states must develop their own rules for violations without specific administrative fines mentioned in the regulation. Additionally, individuals have legal remedies against companies for violations of GDPR.

Key GDPR Requirements

PRIVACY PROGRAM MANAGEMENT

Accountability and Governance

GDPR requires technical and organizational measures demonstrating compliance with the regulation (e.g., training, internal audits of processing activities, corporate privacy policies, codes of conduct and certifications). Additionally, companies must implement "privacy by design" measures that demonstrate the incorporation of privacy and data protection considerations into processing activities.

Data Protection Officers

Companies with significant monitoring or data processing activity must appoint a data protection officer (DPO). The DPO is responsible for advising the company on GDPR and data protection obligations, monitoring compliance with these requirements, and serving as a liaison to supervisory authorities and individuals whose data is processed by the company.

Data Protection Impact Assessments

Companies must assess associated privacy risks when investing in or using new technologies or when processing personal data will likely create a high risk to the rights and freedoms of individuals. Data protection impact assessments provide a structured tool to evaluate and address risks early, as well as provide documentation of compliance activities.

Data Breach Notification

GDPR imposes data breach notification obligations for the first time in the EU. Companies must notify supervisory authorities and affected individuals of breaches that could result in risks to rights and freedoms of the individuals. Breaches need to be reported to supervisory authorities within 72 hours of discovering the incident.

Key GDPR Requirements *(continued)*

DATA PROCESSING AND USE

Lawful Processing

To lawfully process personal data under GDPR, companies must now identify a legal basis for the activity. Lawful processing conditions include:

- Consent of the individual
- Performance of a contract with the individual
- Compliance with legal obligations
- Protection of vital interests of the individual
- Legitimate interests pursued by the controller or a third party (except when overridden by rights or freedoms of the individual)

Cross-Border Data Transfers

GDPR limits the ability of a company to transfer EU personal data outside of the EU, unless such transfers comply with specific safeguards (e.g., agreements between public authorities, binding corporate rules, contractual clauses authorized by a supervisory authority). There are several exceptions to this prohibition, particularly where a company has an individual's informed consent to transfer the data.

Data Subject Consent

To qualify as consent under GDPR, the individual must make some affirmative action (e.g., ticking a box, clicking "accept") that can be documented and verified. Consent under GDPR requires the individual to take some action to confirm consent. Individuals may withdraw their consent at any time.

Data Subject Rights

GDPR both strengthens existing data subject rights, as well as introduces new ones. Specifically, under GDPR, individuals have the right to:

- Be informed of how their data will be used
- Access their data and confirm it is being processed
- Rectify or correct inaccurate or incomplete data
- Request their data be removed or deleted
- Restrict the processing of their data
- Port their data to different services or IT environments
- Object to the use of their data
- Not be subject to a decision based on automated processing of their data that results in a legal or similarly significant effect

CYBERSECURITY AND PRIVACY

MICHAEL P. HINDELANG CIPP/US, CIPM
313.465.7412
mhindelang@honigman.com

KARL A. HOCHKAMMER CIPP/US
313.465.7582
khochkammer@honigman.com