WILLKIE FARR & GALLAGHER LLP

NEW YORK WASHINGTON HOUSTON PARIS LONDON FRANKFURT BRUSSELS MILAN ROME

GDPR: Compliance & Best Practices

Daniel Alvarez
November 1, 2018

WILLKIE FARR & GALLAGHER LLP

Introduction

- Since 1995, data protection in the EU has been governed by Directive 95/46/EC ("the Directive") which instructed Member States to pass their own data protection laws
- In April 2016, the European Parliament passed the General Data Protection Regulation ("GDPR") which went into effect May 25, 2018
- GDPR Goals:
  - Promote uniformity of data privacy laws within the EU
  - Protect EU citizens from data breaches and provide increased control over personal data
  - Change organizational approaches to data security
- GDPR effects:
  - Onerous new burdens for companies that collect or process EU citizens' personal data, regardless of location (extremely broad, extraterritorial scope)
  - Confers broad rights on data subjects
  - Violations can result in massive fines

GDPR Scope

- **Broad scope of data covered**
  - Broad definition of “personal data” protects data that is not typically protected by U.S. privacy laws
  - Pseudonymized data typically is not considered “personal” under U.S. law, but is considered “personal” under GDPR.
  - Publicly available data is “personal data” and protected by GDPR.
  - GDPR does not distinguish between data a company collects from customers and data a company collects from employees.
- **Broad territorial – arguably extraterritorial – scope**
  - Covers data collection/processing of EU-based entities, regardless of where the collection and processing happens.
  - Covers data collected from EU-based data subjects, regardless of whether the data collector/processor is EU-based, if the processor is selling goods and services in the EU or monitoring behavior in the EU.

GDPR Highlights

- **Key Terms**
  - Data Controller: Entity that determines the purposes, conditions, and means of processing personal data
  - Data Processor: Entity that processes data on behalf of the data controller
  - Data Subject: The person whose data can be directly or indirectly identified
  - Supervisory Authority/Data Protection Authority ("DPA"): EU Member State authority to whom a company is accountable for GDPR compliance (e.g. UK Information Commissioner's Office)
  - Data Protection Officer ("DPO"): Independent expert in the field, appointed to advise and monitor GDPR compliance, liaise with DPA, and to act as a point of contact for data subjects

GDPR Highlights

- **Penalties**
  - Potentially quite severe
  - Two tiers depending on severity of GDPR infringement
    - Minor violations: Maximum fine of **€10 million or 2%** of prior year's global turnover (whichever is greater)
    - More serious violations: Maximum fine of **€20 million or 4%** of prior year's global turnover (whichever is greater)
  - Fines and penalties also possible under laws of particular EU Member States
- **Recent Developments**
  - Article 29 Working Party has issued several implementation guidelines
    - "Data Portability," "Data Protection Officers," "Lead Supervisory Authority"
  - UK's Information Commissioner's Office and other national DPAs have published some guidance documents and others pending
  - Germany passed federal statute aligning German laws with GDPR

GDPR Requirements

Notice

- **Requirements**
  - Longer and more detailed than previously required
    - E.g., what data is being processed, why it is being processed, who is doing the processing, data subjects' rights, whether it might be transferred internationally
  - Must be clear, concise, and easily understood
- **Moving Forward**
  - Review all current privacy notices and public-facing documents, and determine where new information is needed
    - Does the current notice explain the what, why, and who of processing?
    - Are data subjects' rights fully explained?
    - Is there a way for data subjects to contact the entity?
  - Update privacy notices to include newly required information
  - Emphasize language clarity
  - Ensure the new documents are easily accessible to the public

Consent

- **Requirements**
  - Data subjects must affirmatively and unambiguously consent to each specific data processing operation
    - Biggest change from the Directive is that consent must be affirmatively given (i.e., no pre-checked boxes)
  - Must keep records to demonstrate consent
  - Must inform data subjects of their rights to refuse or withdraw consent (may require special processes in employment context)
  - Children under 16 require parental consent (Member States can lower this to 13 years)
- **Moving Forward**
  - Review UK ICO GDPR Consent Guidance
  - Review and update current consent policies
    - Ensure data subjects are prompted for consent for each processing operation or that consent adequately covers all operations
    - Require affirmative action from data subjects
  - Develop and implement robust record-keeping to demonstrate consent

Security

- **Requirements**
  - Data must be processed such that it ensures the "appropriate security . . . using appropriate technical or organizational measures."
    - No prescribed security measures lends greater flexibility but also greater risk of running afoul of regulators
    - "Appropriate security" considers state of the art, cost of security measures, and nature of data being processed
  - Aim is to protect against unlawful or unauthorized processing, accidental loss, damage, or destruction of personal data
  - GDPR encourages both encryption and pseudonymization
- **Moving Forward**
  - Assess current state of data protection
  - Explore different measures to safeguard data
    - Pseudonymization is specifically encouraged in the GDPR, some incentives exist, indicates "appropriate security" measures
    - Encryption may totally remove data from GDPR purview
  - Implement measures designed to quickly restore services in the event of a breach
  - Document analysis.

Service Providers

- **Requirements**
  - Data controllers are responsible for the processors with whom they work
    - Must select processors that sufficiently guarantee compliance with GDPR
  - Service providers are responsible for their own GDPR compliance (e.g., implementing appropriate security)
  - Contracts with service providers and vendors need to clearly delineate the rights and responsibilities of each party regarding data
  - Restrictions on subcontracting
- **Moving Forward**
  - Review contracts with vendors and service providers
    - Pay special attention to limits on data processing activities, notification procedures, responsibility allocations
  - Conduct assessments of vendor/service provider security procedures
  - Implement processes to review new contracts to ensure all requirements are covered

Cross-Border Data Transfer

- **Requirements**
  - Little change from current status
  - Data may only be transferred out of the EU:
    - To an entity pre-approved by the EU as having adequate protection
    - With data subject's unambiguous, affirmative consent after notice of international transfer
    - Subject to specific contractual language (e.g., model clauses)
    - Under sufficient binding corporate rules
    - When the entity is certified by an appropriate body
- **Moving Forward**
  - Transferring data to the U.S. will continue to be difficult
  - Ensure data transfer contracts contain pre-approved contractual terms
    - Clearly delineate rights and responsibilities of each party
  - Review new guidance regarding binding corporate rules

Data Protection Officers ("DPO")

- **Requirements**
  - Only mandatory for data controllers and processors who:
    - As a core activity, systematically and on a large scale monitor individuals
    - Process special categories of personal data on a large scale
  - DPOs should be experts in data protection law and practices, able to conduct tasks independently
  - Responsible to advise and assist entity on GDPR compliance, assist with DPIAs, monitor compliance, act as point of contact for the public and lead supervisory authority
- **Moving Forward**
  - WP29's DPO Guidance publication
  - Conduct initial DPIA and determine whether DPO is necessary
  - Decide what type of DPO to hire:
    - Internal
    - External
    - Joint
  - Begin search for DPO

Breach Notification

- **Requirements**
  - First time data breach notification required by EU-wide law
  - Must notify appropriate national DPA within 72 hours of breach
  - If data subjects may be at high risk of harm, personal notification required
    - Certain information must be included, e.g., potential risks, steps being taken to mitigate harm
  - Processors must notify controllers if they suffer a breach
- **Moving Forward**
  - Given short response time, must have processes in place and practiced
    - Develop data breach response plan
    - Have response team predesignated
    - Maintain updated records to ease/speed notifications

Willkie Farr Contacts

Daniel K. Alvarez

Partner
T: 202 303 1125
E: dalvarez@willkie.com

Daniel K. Alvarez is a partner in Willkie's Communications & Media Department in Washington. He is also a member of the Cybersecurity and Privacy practice. Mr. Alvarez brings an extensive background in technology and regulatory issues to counseling a broad range of clients in diverse industries on privacy and cybersecurity issues, including financial and healthcare privacy, regulation of marketing and advertising practices, international data transfer, children's privacy, and other privacy and cybersecurity matters regulated by the FTC, FCC, SEC, and other state and federal agencies.

Mr. Alvarez is a former legal advisor to Federal Communications Commission Chairman Tom Wheeler. As one of Chairman Wheeler's chief advisors, Mr. Alvarez oversaw and advised on the development of policy on some of the highest-profile issues before the FCC, including broadband competition and deployment, privacy, cybersecurity, and public safety.

Prior to joining the FCC, Mr. Alvarez practiced in Willkie's Washington office, advising domestic and international clients in the technology, communications and media industries on a range of issues before state and federal regulatory authorities, including the FCC, Federal Trade Commission, Department of Justice and Department of the Treasury.