McGrath | North

GDPR One Year Later: Today's Impact on US Companies and the Data Privacy Outlook for the Future

7th Annual Corporate Counsel Forum
May 31, 2019

Stacey Shadden
(402) 633-9591
sshadden@mcgrathnorth.com

Agenda

- General Data Protection Regulation (GDPR)
- What is GDPR?
- How does GDPR get jurisdiction over the operations of US companies?
- If GDPR applies to my company, how do I comply?
- How to navigate the day to day operating impacts of GDPR?
- What are the penalties associated with non-compliance?

- US Privacy Laws
- What is the Privacy Shield?
- Current state of US data privacy laws?
- What is the California Consumer Privacy Act?

- Wrap-Up
- One year later, how has GDPR influenced global data privacy?
- What to keep on your radar for the future?

What is GDPR?

- Comprehensive set of data protection regulations that standardizes data protection rules across the entire EU.
- Effective on May 25, 2018.
- Designed to empower data subjects with enforceable rights with respect to how their person data is used, collected and managed.
- “Implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk to personal data.”
- Global impact.

Principles of GDPR

- Lawfulness, fairness and transparency.
- Purpose limitation.
- Data minimization.
- Accuracy.
- Storage Limitation.
- Integrity and confidentiality.

How Does GDPR Apply to US-based Entities?

- Established in the EU (activity through stable arrangements (i.e., office / EE's)).
- Offer goods or services to EU residents (does not have to be a financial transaction).
- Monitor the behavior of EU residents.

Offering Goods and Services?

- Company must show intent to draw EU data subjects as “customers”.
- Company website or access to Company email address or contact information (by itself) is not enough.

Monitoring Behaviors?

- Tracking individuals on the internet and use of personal data to profile or analyze and predict preferences, behaviors and attitudes.
  - Analyzing economic situation, health, personal preferences, interests, location.
- Use of web analytics, tracking, cookies identifiers, geo-location tracking.

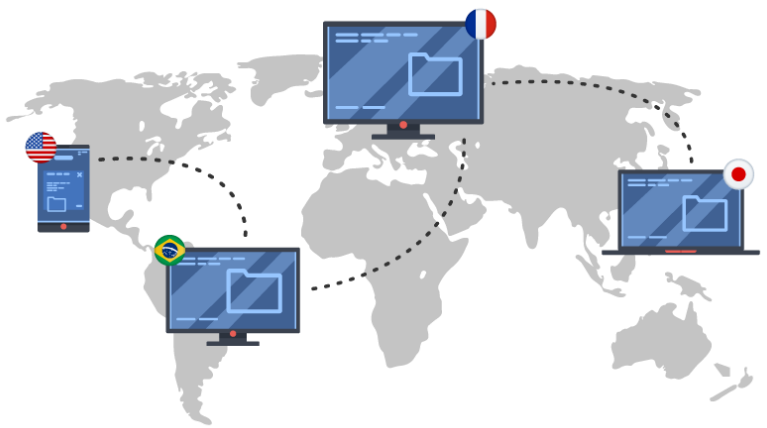
Determining Extent of GDPR Application

- GDPR has a global reach and applies to any business that "processes" or "controls" personal data of any EU citizen.
  - "**Data Controller**" – a company that determines the purposes and means of how personal data will be processed. For example, all companies are data controllers with respect to employee data.
  - "**Data Processor**" – processes personal data on behalf of a controller (i.e., a service provider who you give access to personal data).
  - "**Processing**" – "any operation or set of operations which is performed on personal data or on sets of personal data". Includes: collection, recording, organizing, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure, transmission or destruction.
  - "**Personal Data**" – "any information relating to an identified or identifiable person". Includes: name, an identification number, location data, an online identifier, or one or more factors specific to physical, physiological, genetic, mental, economic, cultural or social identity of a natural person, cookies (if linked to an identifiable person).
    - Note, there are special rules for processing certain kinds of data (i.e., race, ethnicity, religion, sexual orientation, genetic data, etc.)

Even if your company is not required to comply directly with GDPR, consider whether your company is impacted as a data processor of a data controller that is required to comply with GDPR.

Transferring Data Outside the EU

- GDPR permits the transfer of personal data outside the EU subject to the satisfaction of certain conditions:
  - Country whose legal regime is deemed to provide an “adequate” level of personal data protection.
  - Transfers by way of appropriate safeguards:
    - Standard contractual clauses
    - Privacy Shield



How to Comply?

- Data Controller versus Data Processor.
- Privacy Policies (different from US requirements).
- Purpose limitation; data minimization.
- DPO and/or EU Representative.

How to Comply?

- EU resident “rights”
  - Consent
  - Informed
  - Object
  - Erasure
  - Access
  - Portability

Day to Day Impact of GDPR

- Governance
  - Polices and Procedures
    - Update privacy policy and cookie notice
    - Consent procedure
    - Compliance controls
    - Training
  - Record Management and Retention
  - Impact Assessments
    - Data mapping
    - Mitigation tools to limit risk

Day to Day Impact of GDPR

- Information Security Measures
  - Data breach obligations
  - Policies
  - Mitigation
- Third Parties (who is liable?)
  - Vendors
  - Subcontractors
  - Customers

Penalties

- Civil and administrative penalties.
  - Two-tiered structure:
    - Up to greater of $10MM Euro or 2% of company's worldwide annual turnover.
    - Up to greater of $20MM Euro or 4% of company's worldwide annual turnover (more serious offenses).

Penalties

- Criminal penalties (if enacted by a country's local laws).
- Damages in privacy lawsuits by supervisory authorities and data subjects (right expressly granted in GDPR).

Privacy Shield

- Framework governing the flow of data between the EU and the US for commercial purposes.
- Companies self-certify to the US Department of Commerce.
- Adhere to 23 principles laying out the requirements for the use and treatment of personal data received from the EU.
- Deemed to provide “adequate” privacy protection to personal data transferred outside of EU.
- Privacy Shield currently under scrutiny in EU.

US Data Privacy Law

- State specific requirements.
- Federal regulations (GLBA, HIPPA, FERPA, COPPA).

CCPA

- Passed in June 2018; takes effect on January 1, 2020.
- Includes detailed disclosure requirements; grants extensive rights to individuals to control their data; includes statutory fines and a private right of action.

CCPA Applies To:

Either:

A. For-profit business that (1) does business in the state of CA; (2) collects CA consumer personal information; (3) determines the purpose and means of processing the information; and (4) meets one of the following:

   i. At least $25MM in annual gross revenues;

   ii. Buys/sells/shares/receives information of at least 50K CA consumers; or

   iii. Derives at least 50% of annual revenue from selling CA personal information.

OR

B. You control or are controlled by an entity that meets the above criteria and share common branding with that entity (i.e. you don't do business in CA, but your corporate group does).

CCPA Take-Away Points

- Restrictions are similar in some ways, and different in others, to GDPR.
  - Day to day operations
  - Third party service providers
- Generally, nonprofits are not required to comply with CCPA.

Impact of GDPR – One Year Later

- Los Angeles Times (and other US based news sites) - Restricted access to EU users
- Google; Facebook
  - Penalties ($60MM – lack of transparency and consent; $650K)
  - Google's new option to delete location and search histories (auto clears browsing)
- Polish Data Processor - $220K for data scraping
- Portugal Hospital - $400K lack of safeguards to protect patient records
- German Social Media Platform - $20K – data breach (hacker stole and published passwords)
- Austrian Retail Company - $4,800 – lack of transparency and consent

What the future holds?

- As of early 2019, Austria's DPA had 115 US proceedings pending and another 58 investigations underway.
- Irish DPC sited that it had 51 "significant investigations" underway, 12 of which target American companies (a number of investigations to conclude in summer 2019).
- FTC assessed penalties
  - Rumors of potential multi-billionaire dollar fine against social media giant (largest fine to date from 2012 - $22MM)
- Numerous bills with respect to data privacy and consumer rights have been introduced in Congress.

McGrath | North

Stacey A. Shadden
P: 402.633.9591
sshadden@mcgrathnorth.com

McGrath North Mullin & Kratz, PC LLO
1601 Dodge Street | First National Tower | Omaha, NE 68102
www.mcgrathnorth.com