The State of Privacy & Data Security Compliance

Nicole P. Moriarty *and* K. Jon Breyer

KUTAKROCK
kutakrock.com

Overview

KUTAKROCK

Privacy Issues Touch All Types of Operations

- Customer Transactions
  - Data assets
  - Privacy policy review
- HR / Employee
  - Health information
  - Device tracking
  - Biometric
- Information Technology (IT)
  - Network security
- Financial
  - Highly sensitive information
  - PCI

Privacy Compliance Landscape

- U.S. operates under a patchwork of P&DS laws
  - FTC (UDAP)
  - Industry specific laws
  - Various state laws
- International laws starting to have broader reach (GDPR)
- Recent developments (response to GDPR)
  - CaCPA and other state level activity
  - Comprehensive federal proposals

What is Typically Addressed by Data Privacy Laws?

- What information can be collected
- How it can be used
- How it must be protected
- When it can be shared or disclosed
- Requirements for responding to data breaches and data losses
- Penalties for data breaches and data losses

Privacy Law Trends

- Increased transparency
- More individual rights and control
- Expanding view of "personal information"

- All lead to more compliance obligations and more risk
  - Legal risk
  - Reputational risk
  - Economic risk

Significant Developments

KUTAKROCK

What is the EU General Data Protection Regulation (GDPR)?

- The General Data Protection Regulation is an EU Regulation that protects
  - Processing of personal data
  - Free movement of personal data
  - Fundamental rights and freedoms of persons
- European Committee's Goal - One Single Regulation for the EU
- The GDPR offers a new framework for data protection with increased obligations for organizations, and its reach is far and wide
- Replaces the EU 95/46 EC Directive
- Potential fines – 4% annual global turnover or 20 million Euros whichever is higher
- **Enforcement date – 25 May 2018**

KUTAKROCK

Who and What Does GDPR Apply To?

- Who does GDPR apply to?
  - It applies to organizations located within the EU processing Personal Data
  - It applies to organizations located outside of the EU if they offer goods or services to EU citizens or residents
  - It applies to organizations who monitor the behavior of, EU citizens or residents
- What does GDPR apply to?
  - GDPR may apply to an organization if:
  - It offers goods or services to individuals
  - It monitors the behavior of individuals
  - It has employees in EU

California Consumer Protection Act (CCPA)

- **What Businesses are Affected?**
  - Has annual gross revenues in excess of $25 million
  - Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; OR
  - Derives 50 percent or more of its annual revenues from selling consumers' personal information
- Collects consumers' personal information
- Determines the purposes and means of the processing of consumers' personal information
- Does business in California

CCPA – Basic Rights

Four basic rights in relation to their personal information:

- the right to know, what personal information a business has collected about them, where it was sourced from, what it is being used for, whether it is being disclosed or sold, and to whom it is being disclosed or sold;
- the right to "opt out" of allowing a business to sell their personal information to third parties (or, for consumers who are under 16 years old, an opt-in requirement);
- the right to have a business delete their personal information; and
- the right to receive equal service and pricing from a business, even if they exercise their privacy rights under the Act.

CCPA – Penalties

- Any person, business, or service provider that violates the CCPA shall be subject to an injunction and be liable for a civil penalty of not more than $2,500 for each violation or $7,500 for each intentional violation.
- In addition, after satisfying certain procedural requirements, a consumer can bring a civil action for security breaches.

Other Comprehensive Privacy Laws & Proposals

- State-level momentum for comprehensive privacy bills is at an all-time high
  - As of June 4, 2019: 17 states have proposed legislation setting forth a comprehensive approach to governing the use of personal information
    - CA, CT, HI, IL, LA, MD, MA, MN, NV, NJ, NM, NY, ND, PA, RI, TX, WA)
  - Common themes – individual rights (e.g., access, deletion, opt-out), private rights of action, expanded transparency requirements, prohibitions on discrimination
  - Outliers – opt-in requirements; purpose and processing limitations; risk assessment requirements
- Multiple federal proposals
  - Approaches – empowering the FTC – including rulemaking authority and administration of a national DNT list; focusing on certain types of info – web history, GPS, etc. – and certain types of businesses – e.g., ISPs and social media platforms; certifications and penalties; prohibitions on discrimination
  - Preemption potential (not certain)

Managing Compliance

Practical Advice

- Risk assessments
- Consider a scalable approach
  - Maintaining data inventories and managing individual rights
  - Implementing vendor management programs
  - Providing ongoing training
- Data minimization
- Culture and privacy by design
- Cyber insurance

Issue Spotting

- What information are you collecting and why?
- How are you communicating your information practices to your customers? Employees?
- Who has access to the personal information you collect? Who do you share it with?
- Who is responsible for privacy and security requirements?

Kutak Rock | Privacy & Data Security

WASHINGTON, D.C.

Nicole P. Moriarty

202.828.2446
nicole.moriarty@kutakrock.com

MINNEAPOLIS

K. Jon Breyer

612.334.5057
jon.breyer@kutakrock.com