Overview of Key E.U. and U.S. Privacy and Cybersecurity Laws

Brett Lockwood
Smith, Gambrell & Russell, LLP
May 15, 2018

SGR 125th Anniversary
SMITH, GAMBRELL & RUSSELL, LLP

Agenda

- Principal Obligations Under GDPR
- Key U.S. Privacy & Cybersecurity Laws
- E.U. / U.S. Comparison
- Evolving Compliance & Risk Management Practices

Summary

- GDPR effective May 25, 2018
- Broad scope / very process oriented
- Builds on Privacy Directive, with many new provisions, including enhanced personal rights, affirmative consent, data breach notice and DPO requirements
- Penalties – greater of €20 MM or up to 4% of worldwide revenue

GDPR Obligations

Major Requirements

- Privacy by Design Principles
- Notice to EU individuals of data collection practices
- Informed affirmative consent needed to process data if no other lawful basis (e.g., “legitimate interest”)
- EU individuals have right to access, correct and request erasure of data and withdraw consent
- Must implement technical and organizational measures to safeguard personal data

GDPR Obligations

Major Requirements

- Contractors handling data (processors) must adhere to contractual clauses (of controllers)
- Data breach notice within 72 hours to supervisory authorities (without undue delay to individuals)
- Companies with large scale processing or monitoring of personal data must have a data protection officer
- Personal data transfers outside the EU only allowed where adequate level of protection assured

  -- Model clauses, BCRs, U.S.-E.U. Privacy Shield

Federal Level

- No overarching law such as GDPR
- More of a sector approach
  - Financial Services, Healthcare, Education, Public Companies and General Business
- Key Agencies: OCC, HHS OCR, SEC, CFPB & FTC

Federal Level

- **FTC filling void for general businesses, such as manufacturers**
  - Focus on policing deceptive and unfair trade practices under the FTC Act
  - Evolving "common law" of privacy
  - Key requirement: reasonable security measures per prevailing industry practices
  - Uncertainty: pending LabMD case

Federal Level

- **U.S.-E.U. Privacy Shield Program**
  - Option for U.S. companies processing data on E.U. data subjects
  - Privacy by design principles (Notice, Choice, Accountability, Security, Data Integrity, Access & Recourse
  - Must post online Privacy Shield Statement
  - Administered by U.S. Dept. of Commerce and self-certified annually

State Level

- **All States, D.C., Puerto Rico, Guam & Virgin Islands have breach notification laws (but many variations)**
  - Scope of PII, Timing, Notice Content, Agency Notices, Encryption Exceptions, Risk of Harm Threshold, Regulated Industries Exemption

- **Thirteen states (AR, CA, CT, FL, IN, MD, MA, MN, NE, NM, OR, RI, TX, UT) impose affirmative data security obligations – must implement reasonable administrative and technical protections**

State Level

- **California**
  - Privacy policy for apps; Notices to online users; Do-not-track disclosure; Access to data disclosures; Erasure requirements
  - Pending ballot initiative: California Consumer Privacy Act – enhanced disclosure and limits on commercial use of personal data (similar to GDPR)
- **New York**
  - Pending: SHIELD Act: Strengthened breach notification and requirements to implement security safeguards; also includes safe harbors
- **Key takeaway: Patchwork of state laws and constant change = Increased compliance costs ($$)**

E.U. / U.S. Comparison

Obligations

	E.U.	U.S.
Privacy by Design	Yes	Limited
Privacy Notices	Yes	Limited
Affirmative Consent	Yes	Limited
Data Breach Notice	Yes	Yes, but looser
Data Protection Officer	Yes	No
Data Access Rights	Yes	Very limited

E.U. / U.S. Comparison

Obligations

(Cont'd)	E.U.	U.S.
Required Security Safeguards	Yes	Yes, for some sectors and states
Data Transfer Restrictions	Yes	Limited
Penalties	Substantial	More modest
Enforcement	Supervisory Authority; Individual actions	Sector agencies and states; Individual actions vary by state


So, What To Do?

Compliance / Risk Management

Evolving Contract Practices

- Arises in many contexts – cloud computing contracts, vendor contracts, M&A reps and warranties, etc.
- More requests for cybersecurity assurances
- Flow downs to vendors and subcontractors
- Audit requirements – SSAE 16 audits and SOC 1 and 2 reports
- A lot of liability shifting – indemnity clauses, liability carve outs

Compliance / Risk Management

Evolving Contract Practices

- Vendors being required to maintain reasonable security controls
- Contracts being updated to include cybersecurity requirements and indemnities
- Data breach insurance becoming more common

Compliance / Risk Management

Administrative Safeguards

- Implement cybersecurity processes and practices that map to applicable law
- Train staff on cybersecurity awareness
- Consider need for chief privacy officer or committee
- Limit data access on a need-to-know basis
- Collect and retain data only so long as needed
- Properly dispose of data when no longer needed (shred, erase, destroy)

Compliance / Risk Management

Administrative Safeguards

- Review and update privacy policies for web and mobile applications and adhere to them
- Prepare breach response plan (and team) in advance
- Maintain IT systems security policy
- Follow relevant industry best practices (such as PCI Data Security Standards for certain online payments)

Technical Safeguards

- Restrict data on, and password protect, mobile devices
- Use encryption for data at rest and in transit
- Implement strong password practices
- Use firewalls and data intrusion detection tools
- Conduct periodic system security assessments and audits (including for vendors)

Questions Comments Follow-up

Brett Lockwood
blockwood@sgrlaw.com
404-815-3674

SGR 125th Anniversary
SMITH, GAMBRELL & RUSSELL, LLP