GDPR Is Here: What to Expect Now?

Brett Lockwood
Smith, Gambrell & Russell, LLP

June 19, 2018

SGR 125th Anniversary
SMITH, GAMBRELL & RUSSELL, LLP

Agenda

Principal Obligations Under GDPR

Related Developments & What's Ahead

E.U. / U.S. Comparison

Compliance & Best Practices

SGR 125th Anniversary
SMITH, GAMBRELL & RUSSELL, LLP

GDPR Obligations

Summary

- E.U. General Data Protection Regulation (GDPR) was effective May 25, 2018
- Replaces 1995 E.U. Privacy Directive, with many new provisions: enhanced personal rights, affirmative consent, breach notice and DPO requirements
- Very broad and process oriented
- Essentially: If you process personal data of a person in the E.U. or processing is in the E.U. or you are a controller or processor in the E.U. then GDPR applies
- Penalties – greater of €20 MM or up to 4% of worldwide revenue

SGR 125th Anniversary
SMITH, GAMBRELL & RUSSELL, LLP

GDPR Obligations

Key Definitions

- **Data Subject:** an identified or identifiable natural person
- **Personal Data:** any information relating to a Data Subject
- **Processing:** any operation which is performed on personal data
- **Controller:** one who determines the purposes and means for the processing of personal data
- **Processor:** one who processes personal data on behalf of a controller

(Art. 4)

SGR 125th Anniversary
SMITH, GAMBRELL & RUSSELL, LLP

GDPR Obligations

Major Requirements

- **Governing Principles for Processing Personal Data (Arts. 5, 24 & 25)**
  - ► **Processing must be lawful, fair and transparent**
  - ► **Processed for specified, explicit and legitimate purpose**
  - ► **Adequate, relevant and limited to processing purpose**
  - ► **Must be accurate and kept updated without delay**
  - ► **Maintained only as long as necessary for processing purpose**
  - ► **Must ensure appropriate security**

SGR 125th Anniversary
SMITH, GAMBRELL & RUSSELL, LLP

GDPR Obligations

Major Requirements

(Continued)

- Affirmative consent from data subject (or guardian) or another lawful basis (e.g., legitimate interest or contract fulfillment) is needed to process data

  (Arts. 6 - 8)
- Must provide notice (with specific requirements) to data subjects about data practices (Arts. 12 - 14)
- Data subjects have right to access, correct, request erasure and have portability of data, restrict processing and withdraw consent (Arts. 15 – 20)

SGR 125th Anniversary
SMITH, GAMBRELL & RUSSELL, LLP

GDPR Obligations

Major Requirements

(Continued)

- Must implement and document appropriate technical and organizational measures to safeguard personal data (if less than 250 employees, exempt from documentation) (Arts. 24, 25 & 32)
- Contractors handling data (processors) must adhere to written contractual clauses (of controllers) (Art. 28)
- Maintain record of processing activities (Art. 30)

SGR 125th Anniversary
SMITH, GAMBRELL & RUSSELL, LLP

GDPR Obligations

Major Requirements

(Continued)

- Data breach notice within 72 hours to supervisory authorities (without undue delay to individuals) (Arts. 33 & 34)
- Processing highly sensitive data is prohibited unless exception and must perform data protection impact assessments (DPIAs); DPIA also needed where a high risk to individuals (Arts. 9, 10, 35 & 36)
- Companies with large scale processing or monitoring of personal data must have a data protection officer (Arts. 37 - 39)

SGR 125th Anniversary
SMITH, GAMBRELL & RUSSELL, LLP

GDPR Obligations

Major Requirements

(Continued)

- **Companies not present in the E.U. that process personal data must appoint a personal representative in the E.U. (Art. 27)**
- **Personal data transfers outside the E.U. only allowed where an adequate level of protection is assured (Arts. 44 – 47, 49)**
  - ► **Model clauses, BCRs, U.S.-E.U. Privacy Shield**

SGR 125th Anniversary
SMITH, GAMBRELL & RUSSELL, LLP

Developments
& What's Ahead

Post-May 25 Enforcement

- Facebook, Google, Instagram and WhatsApp sued on May 25 by NOYB.eu (Max Schrems group) for alleged non-compliance with GDPR
- But quiet so far from supervisory authorities – for various reasons – but some sense of waiting for other shoe to drop
- Effort by entities should be on demonstrating that privacy is taken seriously – avoid egregious violations

SGR 125th Anniversary
SMITH, GAMBRELL & RUSSELL, LLP

Developments
& What's Ahead

Selected Issues In Need of Clarity

- **Who's actually a "data subject"? Just an E.U. resident or citizen or also non-E.U. individuals?**
- **Geographic scope? For example, does GDPR apply to E.U. personal data processed in U.S.?**
- **Enforceability against an entirely U.S. company or a U.S. subsidiary of an E.U. company?**
- **Responsibilities of GDPR representatives in the E.U.?**
- **Effect and availability of GDPR compliance certifications?**

SGR 125th Anniversary
SMITH, GAMBRELL & RUSSELL, LLP

Developments
& What's Ahead

E.U. ePrivacy Regulation

- **Pending: E.U. ePrivacy Regulation (will replace 2002 ePrivacy Directive, as amended)**
- **Will continue E.U. "cookies policy"**
- **Expected to vastly limit unsolicited commercial electronic communications to individuals and tracking, unless opt-in consent is obtained**
- **Substantial penalties similar to GDPR**
- **Possibly effective in late 2018/early 2019**

SGR 125th Anniversary
SMITH, GAMBRELL & RUSSELL, LLP

Developments
& What's Ahead

Evolving U.S. Regulation

- **Federal Level**
  - ► Bills pending in Congress: CONSENT Act; Social Media Privacy Protection and Consumer Rights Act
  - ► FTC and other agencies continue to be more aggressive in enforcement
- **State Level**
  - ► All states, D.C., Puerto Rico, Guam & Virgin Islands have breach notification laws (but many variations)
  - ► 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

SGR 125th Anniversary
SMITH, GAMBRELL & RUSSELL, LLP

Developments
& What's Ahead

Evolving U.S. Regulation

(Continued)

- **California**
  - ► Privacy policy and do-not-track disclosures; access to data disclosures; some erasure requirements
  - ► Pending ballot initiative: California Consumer Privacy Act – enhanced disclosure and limits on commercial use of personal data (similarities to GDPR)
- **New York**
  - ► Pending: SHIELD Act: Strengthened breach notification and requirements to implement security safeguards; also includes safe harbors

SGR 125th Anniversary
SMITH, GAMBRELL & RUSSELL, LLP

E.U. / U.S. Comparison

Principal Obligations

Subject	E.U.	U.S.
Privacy By Design	Yes	Limited
Privacy Notices	Yes	Limited, varies by sector and state
Affirmative Consent	Mostly	Limited
Data Breach Notice	Yes	Yes, but varies widely
Data Protection Officer	Yes	No
Data Access Rights	Yes	Very limited
Data Correction Rights	Yes	Very limited
Data Erasure Right	Yes	Very limited
Marketing Emails	Mostly Opt-In	Mostly Opt-Out

SGR 125th Anniversary
SMITH, GAMBRELL & RUSSELL, LLP


So, What To Do?

Compliance
& Best Practices

Overall Recommendations

- **Determine if a uniform, "lowest common denominator" or a dual approach is desired for personal data of U.S. and E.U. individuals – will you treat them the same or differently?**

- **For full GDPR compliance, must work through and implement applicable GDPR requirements (see above slides 4-9)**

- **Seek to demonstrate that privacy is taken seriously**

SGR 125th Anniversary
SMITH, GAMBRELL & RUSSELL, LLP

Compliance
& Best Practices

Overall Recommendations

(Continued)

- Audit and document data handling processes and related safeguards for reasonableness and ability to address data subject requests and other legal requirements
- Update privacy and data breach policies – both for external and internal uses
- Update service and supply contracts to address vendor issues and customer / client concerns
- Review insurance policies for adequate coverage

SGR 125th Anniversary
SMITH, GAMBRELL & RUSSELL, LLP

Compliance
& Best Practices

Contract Practices

- Require vendors to provide a data protection addendum, timely notices of breaches and similar assurances
- Be prepared to address customer / client requests for similar data protection assurances from you
- Add appropriate indemnities and exceptions to liability caps for data issues
- Require vendors to maintain cyber-liability insurance

SGR 125th Anniversary
SMITH, GAMBRELL & RUSSELL, LLP

Compliance
& Best Practices

Administrative Safeguards

- Train staff on cybersecurity awareness
- Consider need for chief privacy officer or committee (or a DPO for GDPR)
- 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
& Best Practices

Administrative Safeguards

(Continued)

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

Compliance
& Best Practices

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)

SGR 125th Anniversary
SMITH, GAMBRELL & RUSSELL, LLP

Compliance
& Best Practices

Final Thoughts & Takeaways

- **Cybersecurity and data privacy compliance is here to stay and will get tougher.**

- **It's not too late! Many organizations are still catching up on GDPR and related compliance.**

- ***"[T]his is not the end. It is not even the beginning of the end. But it is, perhaps, the end of the beginning." Winston Churchill***

SGR 125th Anniversary
SMITH, GAMBRELL & RUSSELL, LLP

Questions Comments Follow Up

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

SGR 125th Anniversary
SMITH, GAMBRELL & RUSSELL, LLP