SEYFARTH SHAW

What to do for May 25, 2018: GDPR Readiness

Presented by John Tomaszewski and Kathleen McConnell

SEYFARTH SHAW

Seyfarth Shaw LLP

Legal Disclaimer

This presentation has been prepared by Seyfarth Shaw LLP for informational purposes only. The material discussed during this webinar should not be construed as legal advice or a legal opinion on any specific facts or circumstances. The content is intended for general information purposes only, and you are urged to consult a lawyer concerning your own situation and any specific legal questions you may have.

Agenda

01 The “Basics” - Compliance Programs

02 The “New Normal” - Accountability

03 The “Delta” – Differences from Old Law

04 The “Difficult” – Litigation and Transfers

Speakers

John Tomaszewski

Co-Chair Global Privacy and Security Team
Houston Office
jptomaszewski@seyfarth.com

Kathleen McConnell

Global Privacy and Security Team
San Francisco Office
kmcconnell@seyfarth.com

SEYFARTH SHAW

The Basics – What Do You Need for a Compliance Program Already?

Compliance – Administrative Requirements

- Policies
  - Transparency is a foundational principle
  - Consent is now “express”
  - Privacy policies
  - HR policies
  - Vendor management policies
- Technical & Organizational Controls
  - Standard operating procedures
  - Technical controls
- Security
  - The usual suspects
- Breach Notices

Compliance – Administrative Requirements (cont.)

- Processor Contracts
  - Obligations follow the data
- Joint Controller Obligations
  - You may be a controller even if you think you are not
  - Joint & several liability
- Records of Processing
  - Have to keep a “ledger” of what you do with the data
  - How you use it and who you send it to
- Data Protection Impact Assessments
- Cooperation with Regulators (prior consultations)
  - Some processing needs advance approval

Compliance – Business Requirements

- Privacy by Design
  - Need to build privacy into product development
  - Default to the “6 Principles” in design
  - Privacy is everyone’s job – like quality
- DPO Designation & Role
  - Independence
  - Competence
  - Support
  - Location/Language

SEYFARTH SHAW

The New Normal – Accountability

Accountability

- Accountability is “New Normal”
  - Demonstrate compliance
  - Framework needs to work
  - Training
  - Audit
- Presumption of Failure
  - If breach, then € fine?
- Failure to Comply with **Any SINGLE** Element Can Trigger € Fine

Accountability – How Do You Do It?

- Privacy Impact Assessments
  - What is the risk to individual rights in a service
  - Existing features & functionality
  - New processing
- Standard Operating Procedures
- Audit
  - Internal audit processes
  - Third party audits
- Certifications & Codes of Conduct
  - New feature in GDPR

Document Everything

SEYFARTH SHAW

The Delta – What Is Different

Directive v. Regulation

Administrative Changes

- Designation of DPO
- Data Protection Impact Assessments
- Audit Obligations
  - Demonstrate compliance
  - Certifications
  - Codes of Conduct
- Breach Notification
  - Compressed timeframe (72 Hours)
- Privacy By Design
- Contracts, Contracts Everywhere

New or Expanded Rights

- Consent
  - Specific conditions for consent
  - “Express” consent (no more “opt-out”)
- Right to Erasure
  - Force deletion
- Data Portability
  - Individual’s right to take it with them
  - Motivated by social media
  - Impacts a lot more than just social media

Data Transfers

- General Principles for **All** Transfers
  - Can **ONLY** Transfer Subject to Chapter V
    - Limits transfer mechanisms
    - Distinguishes cross-border transfers from other processing
  - Commission Adequacy Decisions
  - Binding Corporate Rules
  - International Agreements (MLAT, etc.)
  - "Appropriate Safeguards"
    - Model Clauses
    - Certifications & Codes of Conduct

SEYFARTH SHAW

The Difficult – Data Transfers in Litigation

Challenges of Data Transfers for Litigation Purposes

- **Organizations are often "between a rock and a hard place" and must choose between violating U.S. discovery orders/subpoenas or violating EU data protection laws**
  - Risk of substantial fines, sanctions, and denial of licenses (greatly increased under GDPR)
  - Risk of criminal sanctions for violation of blocking statutes & data privacy

Background: Differing Notions of U.S./EU Privacy, Discovery, and Civil Justice

- **U.S. – Primary focus**: protect constitutional right to a meaningful "day in court," which requires discovery adequate to help "level the playing field" between parties
  - Paramount to the concern for data privacy and protection.
- **EU – Primary focus:** protecting fundamental individual human right to privacy and data protection, even at expense of restricting discovery/disclosure of key relevant information uniquely in hands of opponent
  - Paramount to the concern for "levelling the playing field" in *David v. Goliath cases*. Genesis is found in history of intrusive surveillance to fuel human rights abuses by Gestapo/Stassi/KGB and similar groups.

Scope of Discovery in the US is Broad, Particularly as Compared to European Jurisdictions

- **US Approach – FRCP 26**: Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case.
- **EU Approach**: The approach of many of the EU/EEC countries is that disclosure of documents is frequently limited (e.g., to documents that would be admissible at trial, or that are very specifically described).

U.S. Courts Have Historically Provided Limited Deference to Competing Privacy Laws

- The Hague Convention on Taking of Evidence Abroad (1970)
  - Provides one method of international discovery (U.S. Supreme Court *Aerospatiale* decision)
  - However, it is subject to numerous drawbacks, including those relating to time, cost, uncertainty of success, and country-specific reservations (i.e., countries who have filed reservations refusing to honor requests for pre-trial disclosure of documents, such as France, Germany, Spain, and the Netherlands)
- Applying the *Aerospatiale* balancing test, U.S. courts frequently conclude that compelling production overseas is warranted

Roadblocks to Production Under the European Regime

- EU Data Protection Directive 95/46/EC and the GDPR are similar in significant ways
  - They both contain restrictions on processing data for reasons other than those stated at the time of collection
  - They both contain restrictions on international transfers of data
- However, there are some notable differences under the GDPR with respect to the availability of exceptions to such restrictions, and the severity of potential sanctions
- Blocking Statutes: France (generally); Switzerland (sector specific), etc.

Select Provisions Regarding Processing and Cross-Border Transfers under the GDPR

- **Processing: Chapter II**
  - Principles regarding Processing Personal Data: Chapter II, Article 5
  - Lawfulness of Processing: Chapter II, Article 6
  - Conditions of Consent: Chapter II, Article 7
- **Transfers: Chapter V**
  - General Principles for Transfers: Chapter V, Article 44
  - Transfers on the Basis of An Adequacy Decision: Chapter V, Article 45
  - Transfers Subject to Appropriate Safeguards: Chapter V, Article 46
  - Derogations for Specific Situations: Chapter V, Article 49

Potential Cross-Border eDiscovery Mechanisms – All Subject to Significant Limitations under the GDPR

- Select Options for Cross-Border Transfer to Non-Adequate Countries:
  - E.U.-U.S. Privacy Shield
  - EU Model Contract Clauses (Chapter V, Article 46)
  - EU Binding Corporate Rules (Chapter V, Article 46)
  - Code of Conduct (Chapter V, Article 46)
  - Approved Certification Mechanism (Chapter V, Article 46)
- Overarching challenge: onward transfer restrictions

Potential Cross-Border eDiscovery Mechanisms – All Subject to Significant Limitations under the GDPR (Con't)

- Options for Cross-Border Transfer to Non-Adequate Countries (con't):
  - Potential derogations for specific situations under GDPR, Chapter V, Article 49?
    - Consent (subject to significant limitations, especially for employees, and sometimes logistically not feasible – e.g., customers)
    - Establishment, exercise or defense of legal claims (however, commonly recognized to refer only to EU legal claims)
    - Compelling legitimate interest – Article 49(1)(g): However, limited to circumstances where the transfer is
      - from a public "register"
      - not repetitive
      - concerns only a limited number of data subjects
      - AND interest is generally defined by Member State law

Balancing Competing Interests

- Raise cross-border discovery issues early in litigation proceedings and meet and confer regarding retention and scope
- Evaluate alternative sources of data
- Consider phased discovery
- Minimize the amount of personal data, limited to what is truly required for the lawsuit
- Review in country
- Anonymize or pseudonymize data
- Ensure entry of a protective order consistent with GDPR requirements
  - Consider how documents will be treated in trial exhibits

Resources

- The Sedona Conference Practical In-House Approaches for Cross-Border Discovery & Data Protection (2016)
- The Sedona Conference International Principles on Discovery, Disclosure & Data Protection in Civil Litigation (Transitional Edition) (2017)
  - Includes Model U.S. Federal Court Order Addressing Cross-Border ESI Discovery
  - Includes Model U.S. Federal Court Protective Order

Sedona Principles

The Sedona Conference International Principles on Discovery, Disclosure & Data Protection in Civil Litigation (Transitional Edition) (2017)

Principle One: With regard to data that is subject to preservation, disclosure, or discovery in a U.S. legal proceeding, courts and parties should demonstrate due respect to the Data Protection Laws of any foreign sovereign and the interests of any person who is subject to or benefits from such laws.

Principle Two: Where full compliance with both Data Protection Laws and preservation, disclosure, and discovery obligations presents a conflict, a party's conduct should be judged by a court or data protection authority under a standard of good faith and reasonableness.

Sedona Principles

Principle Three: Preservation, disclosure, and discovery of Protected Data should be limited in scope to that which is relevant and necessary to support any party's claim or defense in order to minimize conflicts of law and impact on the Data Subject.

Principle Four: Where a conflict exists between Data Protection Laws and preservation, disclosure, or discovery obligations, a stipulation or court order should be employed to protect Protected Data and minimize the conflict.

Sedona Principles

Principle Five: A Data Controller subject to preservation, disclosure, or discovery obligations should be prepared to demonstrate that data protection obligations have been addressed and that appropriate data protection safeguards have been instituted.

Principle Six: Data Controllers should retain Protected Data only as long as necessary to satisfy legal or business needs. While a legal action is pending or remains reasonably anticipated, Data Controllers should preserve relevant information, including relevant Protected Data, with appropriate data safeguards.

SEYFARTH SHAW

Thank You