SEYFARTH SHAW

Which GDPR Requirements Carry the Most Significant Sanctions?

Presented by
John Tomaszewski and Jason Priebe

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 GDPR Penalty Tiers

02 The 2% Penalties – Tier 1

03 The 4% Penalties – Tier 2

04 “Opening Clauses”

Speakers

John Tomaszewski

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

Jason Priebe

Global Privacy and Security Team
Chicago Office
jpriebe@seyfarth.com

SEYFARTH SHAW

The EU General Data Protection Regulation (GDPR) Penalties

The GDPR

- Will enter into force on **May 25, 2018**.
- Dramatically increases penalties for data privacy violations.
- Tiered fines:
  - Tier 1:
    - 10,000,000 Euros or 2% **Global** Turnover
      - For violations in data security, storage, breach, breach notification, trans-border transfers, transparency of information, child consent.
  - Tier 2:
    - 20,000,000 Euros or 4% of **Global** Turnover
      - For violations in data processing, consent, data subject rights, third-party transfers

SEYFARTH SHAW

Tier 1: *The "2% Penalties"*

Article 83(4) of the GDPR - Administrative Fines

- Controller & Processor Obligations
  - Processing of Children's Data
    - Over 16 - may use consent of child
    - 13 to 16 – need consent of parent/guardian
  - Pseudonymous Processing
  - Certification Violations (If Company is Certified Compliant)
  - Compliance Framework Failures

    (Articles 25 through 29)

Compliance Framework Requirements

- Policies
- Technical & Organizational Controls
- Privacy by Design
- Processor contracts
- Joint Controller Obligations
- Records of Processing
- Cooperation with Regulators (prior consultations)
- Security
- Breach Notices
- Data Protection Impact Assessments
- DPO Designation & Role

Compliance Framework Continued

- 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

SEYFARTH SHAW

Tier 2: *The "4% Penalties"*

Article 83(5) of the GDPR - Administrative Fines

- Basic Principles for Processing
  - "Fair & Lawful" processing
  - Purpose Limitation & Data Minimization
  - Accurate and Relevant
  - Retention Limitation
  - Secure
  - Accountable (Demonstrate Compliance)

Article 83(5) of the GDPR - Administrative Fines (Cont.)

- Basis for Processing
  - Performance of Contract
  - Compliance with *EU* Legal Obligation
  - Vital Interest of Individual (think Frist Responders)
  - Public Interest Tasks (defined by EU Member State Law)
  - *GoogleSpain* Balancing Test
- Consent
  - Is Still a Basis for Processing… BUT
  - Article 7 Specifies Conditions
    - Express
    - Free & Informed
    - Revocable

Individual Rights Violations

- Transparency
  - Notice of Practices to Data Subject
    - Even Where No Consent Present
    - Required When Collecting
      - Directly from Data Subject
      - From a Third Party
    - Requirements for Content of Notice
- Access & Correction Rights
- Deletion Rights
- Stopping Processing
- Data Portability
- Right to Object (Used to be “Opt-Out”)
- Automated Processing Opt-Outs

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

Article 49 Derogations

- Allows Transfers Outside Previous Requirements
  - Similar to “Fair & Legal” Basis for Processing
    - performance of contract, public interest, legal defenses or claims, consent, etc.
  - **No Balancing Test**
    - Processing Basis can use Balancing Test
    - Cross Border Transfers MUST use Enumerated Mechanisms or Derogations
  - Derogations as Basis for Transfer MUST be Documented
    - DPIA Maybe?

Article 83(6) Administrative Penalties

- Failure to Comply with Supervisory Authority Orders
  - 4% Penalty
  - On Top of Underlying Penalty Triggering Order
    - Up to 8% of Gross Global Receipts
    - €40,000,000 if you don't have enough in Receipts…

SEYFARTH SHAW

“Openings Clauses” and Associated Penalties

Article 83(5)(d) Administrative Penalties

- The Surprise 4% Penalty
- Any Violation of a Member State Law “Opening Clause”
  - Member States Can Modify GDPR Under Chapter IX
    - Freedom of Expression
    - Public Access to Official Documents
    - National IDs
    - Research
    - Professional Obligations (e.g. Attorney-Client Privilege)
    - Religious Organizations
    - **Labor & Employment Laws**

SEYFARTH SHAW

Penalty Determination

Article 83(2) Criteria

- Not Always “Worst Case”
- Not What is “Commercially Reasonable”
  - Nature, Gravity, and Duration of Violation
  - Intentional vs. Negligent
  - Mitigation Actions & Cooperation with Regulators
  - Prior Violations
  - Type of Data Impacted
  - Degree of Responsibility (Co-Controllers, Processors v. Controllers, etc.)
  - Notification Method (Support Self-Reporting)
  - Certification or Code of Conduct Participation
  - “Other Aggravating of Mitigating Factor Applicable”
    - Whatever the Regulator thinks is important

Privacy Violation Sanctions – Chapter VIII

- Not Just Administrative Penalties
  - €20,000,000 is just the Beginning
  - “Compensation” to Individual
- Judicial Remedies As Well (Liability for Damages & Compensation)
  - Individual Rights of Action
  - Class Actions
  - “Civil Society” Actions
    - Privacy Advocates Suing on Behalf of Individuals
  - Actions Against Regulators to Force Enforcement
- Member States can Add to Penalties (Article 84)
  - “Openings Clauses” can be used to add to fines and criminal sanctions.
  - Judicial Money Remedies (e.g. Tort Law)

SEYFARTH SHAW

Thank You