Morgan Lewis

EU GENERAL DATA PROTECTION REGULATION (GDPR) – IMPACTS ON THE US HEALTHCARE SECTOR

RA Dr. Axel Spies

February 21, 2019

Our Agenda Today

- Broader Territorial Scope of the GDPR, Affecting US Companies
- European Data Protection Board on IFCs
- Data Processing Obligations
- Other GDPR Obligations
- GDPR Sanctions and Penalties

"Beyond EU Borders" → Expanded Scope of the GDPR (Art. 3), compared with the earlier EU laws

GDPR applies directly to data controllers and processors in the US under the following conditions

- Established in the EU ("establishment" is defined broadly) ➞ covered
- No Establishment in the EU but:

  Offering goods or services "to data subjects in the Union" ➞ covered, but mere website access in the EU is **not** sufficient

  Often forgotten: nationality of the data subject does not matter.

  Problem: US subscriber traveling in Europe looks at US website
- US healthcare providers without an EU "establishment" that monitor data subjects (e.g., heart beat, or other vitals through their devices) ➞ covered

Disclosing Personal Data Often Requires Informed Consent - Fair Processing Condition

- Consent is the favorite tool in the healthcare business. However, some GDPR data processing can be based on other grounds:
  - Scientific and historical research (narrowly defined)
  - Necessary for entering into or performing a contract
  - Compliance with a legal obligation to which the data controller is subject
  - Necessary to protect the vital interests of the data subject (= "helicopter" exemption).

Specific "informed" consent required for processing of EU health data ➞ sensitive data under Art. 9 (1) GDPR

Always note: data accesses = data transfer

Don't assume that HIPAA and GDPR consents are identical.

The European Data Protection Board (EDPB) on ICF and GDPR (January 23, 2019)

Some important EDPB findings:

Restrictive approach.

- 'Free' consent means that individuals should have a **real choice and control** →no free consent where there is a 'clear imbalance' between the individual concerned and the organization processing his or her personal data.
- **Specific effort** in case trial patients are **"economically or socially disadvantaged"** or fall under a **"institutional or hierarchical dependency."**
- **Withdrawal** at any time. Withdrawal of will not affect processing operations authorized on **other grounds**.
- Personal data for **other scientific purposes** this is allowed in narrowly defined situations for scientific, historical research or statistical purposes.

➡ "Consent" as legal basis can be risky

Using Third Party Data Processors

- Sometimes difficult to determine who is a "data controller" and who is a "data processor"
- Contracts with such third parties must include provisions in compliance with GDPR if such
  - Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees under the GDPR (Art. 28).
  - The processor shall not engage another processor (sub-processors) without prior specific or general written authorization of the controller.

Co-controller models become more significant (EJC 2018 decisions: Jehovah's witnesses and FB Fanpage)

Selected Processor Obligations

1. Processor must not appoint a sub-processor **without the prior written consent of the controller**. Sub-processors must be subject to flow-down obligations from the processor.
2. Processor is subject to confidentiality obligations and personnel must have same.
3. Processors (and any sub-processors) shall not process personal data, except in accordance with the instructions of the controller, or the requirements of EU law or the national laws of Member States.
4. Recordkeeping obligations
5. Cooperate with Data Protection Authorities
6. Data security obligations
7. Data breach reporting
8. Appointment of a Data Protection Officer (if applicable)
9. Cross border Transfers comply with GDPR rules

Data Processor Contracts: Mandatory Provisions

1. Scope, nature and purpose of processing must be defined
2. Identify types of personal data to be processed
3. Duration of the processing
4. Processes the personal data only on documented instructions from the controller
5. Data security obligations must be addressed
6. Processor must assist controller in meeting its obligations regarding data breaches

Data Processor Contracts: Mandatory Provisions (cont'd)

7. Processor must assist controller in satisfying requests from data subjects
8. Processor must return or delete personal data at end of contract
9. Demonstrate compliance with all of the obligations imposed by the GDPR
10. Allow the controller to perform compliance audits
11. Consent of the controller is required if processor uses a sub-processor
12. Flow-down obligations imposed on sub-processor
13. Independent obligation to inform the controller if, in its opinion, the controller's instructions would breach Union or Member State law

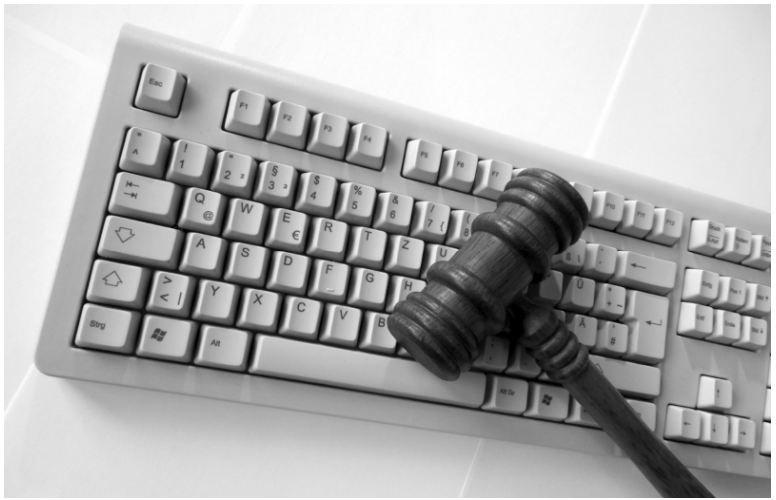
Data Breach Under the GDPR: Controllers/Processors

- "Personal data breach" is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, **personal data** transmitted, stored or otherwise processed."
- In the event of a breach, GDPR requires:
  - ✓ Notification to the Supervisory Authority;
  - ✓ Without undue delay, and where feasible **no later than 72 hours**; and
  - ✓ May also trigger notification obligations to affected data subjects
- **Important Exception**: No notification required if the "personal data breach is unlikely to result in a risk for the rights and freedoms of natural persons"

Take this obligation serious: Non-compliance can trigger large DPA penalties, processors must inform their controllers

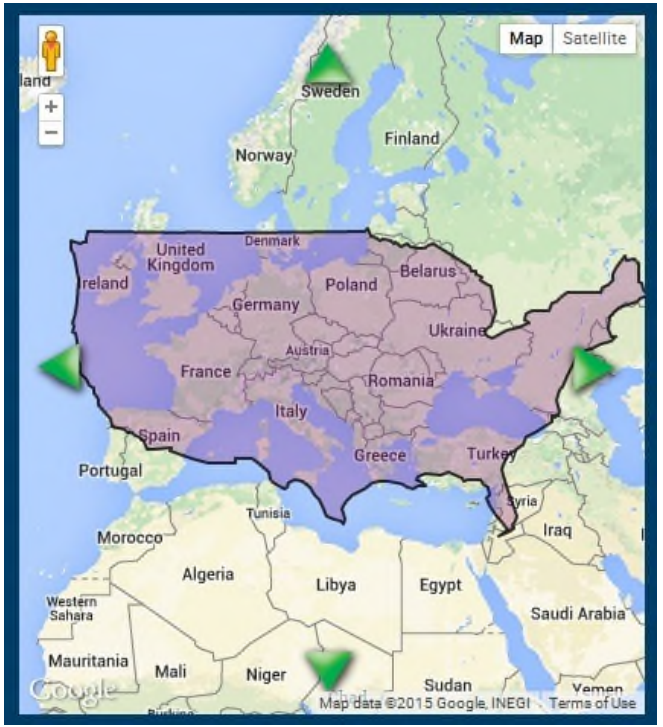
Other GDPR Compliance Obligations

- Data Protection Officer – applies to controllers and processor
- Appointing a Representative in the EU (if there is no "establishment")
- Recordkeeping requirements – Imposed on controllers and processors
- Data security
- Data protection by design
- Data protection by default
- Codes of conduct and certification mechanisms
- Data protection impact assessment



Cross-Border Transfers and the GDPR

- GDPR restricts transfers of personal data outside the EU
- Allowed if:
    1. Adequacy Decision
    2. Binding Corporate Rules
    3. Standard Contractual Clauses
    4. Certifications
    5. Approved Code of Conduct
    6. *Ad Hoc* contractual clauses
    7. Explicit consent from the data subject
    8. Privacy Shield



EU-US Privacy Shield (PS) – What Is It?

- Necessary because of European Court of Justice's (ECJ's) "Schrems" decision of Oct. 6, 2015 (C-362/14), striking down EU-US "Safe Harbor"
- Available since August 1, 2016 – Privacy Shield Framework
- Voluntary – U.S. data importers can self-testify with US Department of Commerce
- Covers many, but not all, EU-US data flows
- Enforced by FTC/DOT
- Public Privacy Shield register with statements of approved data importers
- Complicated dispute resolution mechanism

Fines and Penalties Under the GDPR

- The GDPR has two tiers of Penalties for Non-Compliance – the GREATER of:
  1. €20 million or 4% of global turnover; or
  2. €10 million or 2% of global turnover
- Imposed by the DPAs, can be challenged in court
- Damages can be awarded by courts to data subjects
- Criminal liability – not specifically provided for in the GDPR but possible if an EU member state enacts such rules

Fines and Penalties Under the GDPR (cont'd)

France:

- CNIL fine of $57 million; 01/21/2019: lack of transparency, lack of informed consents by data subjects

Portugal:

- $400,000 for data access

Germany:

A total of 41 fines have reportedly been issued for GDPR violations by the DPA of the various German states so far.

Range €20,000 to 40,000

Fines and Penalties Under the GDPR (cont'd)

Violations → examples:

- A clinic accidentally handed over a copy of a severely handicapped person's ID card to the wrong patient.
- Bank customers were able to see the bank statements of third parties in online banking.
- Web shop customer data was copied without authorization following a hacker attack.

GDPR Enforcement Risk by Regulators in the EU

- What to expect from the EU regulators (DPAs)?
  - Staffing issues at the EU regulators
  - Potential "high-value" targets?
  - Future role of the lead DPA (Art. 60) and mutual assistance (Art. 61)
  - Future role of the new EU Data Protection Board (Art. 64, 65, 68).

GDPR Enforcement Risk: Private Litigation

- **Legal Basis for Individual Lawsuits :** Art. 82 (1) GDPR: "*Any person who has suffered material or non-material damage as a result of an infringement of this Regulation [GDPR] shall have the right to receive compensation from the controller or processor for the damage suffered.*"
- **What is covered?** All individual rights under the GDPR, such as
  - Documentation obligations (Art. 30)
  - Obligations to delete and correct data (Art. 16, 17)
  - No, false or late notification of a data security breach (Art. 32)
  - Violation of the information rights benefitting the data subjects (Art. 12)

Thanks!

Dr. Axel Spies
Washington, DC
+1.202.739.6145
axel.spies@morganlewis.com
Click Here for full bio

Dr. Axel Spies has advised clients for many years on various international issues, including licensing, competition, corporate issues, and new technologies such as cloud computing. He counsels on international data protection (EU General Data Protection Regulation), international data transfers (Privacy Shield), healthcare, technology licensing, e-discovery, and equity purchases. He is a co-publisher of the German Journals ZD (Journal of Data Protection and MMR (Multimedia Law) and a co-author on two GDPR-related handbooks.

Join us next month!

Please join us for next month's webinar:

Fast Break: NRC Regulation and Enforcement in Healthcare

Featuring Lewis Csedrik, Stephen Burdick, Roland Backhaus

March 21, 2019 3:00 PM (EST)