



FOLEY
HOAG AARPI

The New EU General Data Protection Regulation: What It Means For US Healthcare/Life Science Companies

Catherine Muyl, cmuyl@foleyhoag.com
Colin Zick, czick@foleyhoag.com
Marion Cavalier, mcavalier@foleyhoag.com

MichBio Webinar – March 13, 2018



Catherine Muyl, Partner

Foley Hoag, Paris

+33(0) 1 73 02 69 13 | cmuyl@foleyhoag.com



Colin Zick, Partner

Foley Hoag, Boston

617-832-1275 | czick@foleyhoag.com



Marion Cavalier, Associate


Foley Hoag, Paris

+33(0) 1 73 02 69 12 | mcavalier@foleyhoag.com

Cultural gap between the EU and the US



Why should you care about those rules?

- GDPR is « general » i.e. it applies to all activities including the Healthcare / Life Sciences.
- As of May 2018: Supervisory Authorities can impose administrative fines of up to:
 20 million Euros, or 4% of total worldwide turnover of the preceding financial year, whichever is higher.



Who has to comply?

Now

- Controller has an establishment in the EU; or
- Controller uses equipment, automated or otherwise, situated in the EU.

As from May 2018

- Controller or processor established in the EU; or
- Controller or processor not established in the EU where processing activities relate to:
 - the offering of goods or services in the EU; or
 - the monitoring of data subjects in the EU.

What kind of data is covered?

■ Personal Data

Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to his the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. [operative as from May 2018]

What kind of activity is covered?

■ Processing

Any operation or set of operations which is performed upon on personal data or on sets of personal data, whether or not by automatic automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking restriction, erasure or destruction. [operative as from May 2018]

Sensitive data (« special categories of personal data »):

- Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, [...] genetic data, biometric data for the purpose of uniquely identifying a natural person data concerning health or data concerning a natural person's sex life or sexual orientation. [operative as from May 2018]

Controller:

- The person or body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Processor:

- The person or body which processes personal data on behalf of the controller.

Lawfulness of processing

- To be lawful, the processing of personal data (other than sensitive data) must be based on one of the following **legal grounds**:
 - consent / necessary for the performance of a contract / necessary for compliance with a legal obligation / vital interests / public interest / legitimate interests.

- The processing of sensitive data is **prohibited except if based on the following**:
 - explicit consent / vital interests / employment / preventive or occupational medicine based on EU law or pursuant to contract with a health professional / archiving, scientific or historical research purposes or statistical purposes...

Requirements for a valid consent

MUST BE

- ✓ Given by a statement or clear affirmative action
- ✓ Freely given, specific, informed and unambiguous
- ✓ Proven by the data controller
- ✓ Withdrawn as easily as it is given
- ✓ Additionally for sensitive data (incl. health data) **explicit.**

MUST NOT

- ✗ Be inferred from silence, pre-ticked boxes or inactivity
- ✗ Make consent a condition for receiving a service
- ✗ Use confusing, unclear language
- ✗ Be bundled with other terms and conditions

How to draft my (explicit) consent forms?

- Consent must be informed, therefore the following minimum info should appear in the form:
 - ❑ the controller's identity,
 - ❑ the purpose of each of the processing operations for which consent is sought,
 - ❑ what (type of) data will be collected and used,
 - ❑ the existence of the right to withdraw consent,
 - ❑ information about the use of the data for decisions based solely on automated processing, including profiling.

- Consent must be given in a granular and specific way
 - ❑ We advise a tick box for each purpose

- Is it mandatory to have a written and signed form?



EU Data Subjects' Rights

- Information
- Access
- Rectification
- **Erasure (« right to be forgotten »)**
- Restriction
- **Data portability**
- Objection



Exemptions for Scientific Research

■ Scope

- Apply to organizations that process personal data **for scientific research purposes** as long as they implement appropriate safeguards which include “technical and organizational measures to ensure data minimization”.

■ Exemptions to some of the **Data Subjects’ Rights**

- Right to information and access / right to be forgotten / right to object

■ Broader **consent**

■ **Further processing** allowed



Agreements between Controllers and Processors

- Heavier obligations and liabilities for processors.
- Contracts between controllers and processors are now mandatory and must include:
 - the subject matter and duration of the processing;
 - the nature and purpose of the processing;
 - the type of personal data and categories of data subjects;
 - the obligations and rights of the controller;
 - a list of minimum terms, obligations of the processors to ensure that both the controller and the processor comply with GDPR.

Representative

- Controllers and processors not established in the EU must appoint a representative in the Union.

Data Protection Officer

Must be appointed by controller and processors where :

- Processing is carried out by a **public** authority or body; or,
- Core activities consist of processing operations which by virtue of their nature, their scope and/or their purposes, require **regular and systematic monitoring of data subjects on a large scale**; or,
- Core activities consist of **processing on a large scale of sensitive data**.

Mandatory Record

- Obligation to maintain a **record of processing activities** containing the answers to the following questions:
 - Who?
 - Where?
 - What?
 - Until when?
 - Why?
 - How?

Data Protection Impact Assessment

- Required where a processing likely to result in a high risk to the rights and freedoms of natural persons, for example:
 - processing on a large scale of sensitive data (**including health data**),
 - systematic monitoring of a publicly accessible area on a large scale (in particular CCTV),
 - automated processing on which decisions are based that produce legal effects.

Transfers to countries which do not provide an adequate level of protection (including the US) :

- Current transfer tools :
 - to the US : Privacy Shield.
 - Standard Contractual Clauses (SCC) issued by the Commission.
 - Binding Corporate Rules.
 - Consent.

- Additional transfer tools as from May 2018:
 - SCC issued by a Supervisory Authority.
 - Code of Conduct approved by the Supervisory Authority with binding and enforceable commitments from data importer.
 - Certification with binding and enforceable commitments from data importer.

SECURITY, PRIVACY AND THE LAW

LEGAL PERSPECTIVES ON THE EXPANDING UNIVERSE OF INFORMATION SECURITY & PRIVACY ISSUES

General Data Protection Regulation: What It Means For US Healthcare/Life Science Companies (Part One)

Posted on August 24th, 2017 by Catherine Muyl and Marion Cavalier



This is the first post in a three-part series designed to provide a summary of some of the GDPR features that are likely to have the most substantial impact on healthcare/life science related businesses. (Links for [Part Two](#) and [Part Three](#))

The clock is ticking: on May 25, 2018, in less than a year from now, the General Data Protection Regulation ("the GDPR") will

apply in all Member States of the European Union ("EU") and will replace the [Directive 95/46/CE](#) ("the Directive").

Legal perspectives on the
expanding universe of
information security &
privacy issues

www.securityprivacyandthelaw.com



FOLEY
HOAG AARPI



Thank you!

FOLLOW US: @FoleyHoag