

# Sponsor compliance for non-EU companies

Nico Busch, Ass. Jur.

genae

# Disclosure

Speaker name:

Nico Busch

I have the following potential conflicts of interest to report:

- Consulting
- Employment in industry
- Stockholder of a healthcare company
- Owner of a healthcare company
- Other(s): employment at Contract Research Organization
  
- I do not have any potential conflict of interest

Data Transfer

Data Protection Officer

Data Representative

## Data Transfer

- Chapter V, Art. 44 – 50
- 5 pages (EN)
- + 15 recitals

Data Protection Officer

Data Representative



Source: [gdprtoons.com](http://gdprtoons.com)

# Introduction

GDPR sets up data protection standards

Within a clinical trial:

Processing is done e.g. by someone located in the EU (site) → this is what makes GDPR applicable for clinical trial data (Art. 3 | GDPR).

Non-GDPR-bound controllers (e.g. sponsors) may request to have access to the collected data.



[www.your-trips.de/travelmap.php](http://www.your-trips.de/travelmap.php)

# Data-Transfer outside of the EU

Third Country

Non-GDPR-bound country



[www.your-trips.de/travelmap.php](http://www.your-trips.de/travelmap.php)

# Data-Transfer outside of the EU

Third Country

Non-GDPR-bound country

International Organization

Has an entity in a GDPR-bound country, but also in a third country

Personal data

→ Anonymized data: OK ✓

→ Pseudonymized = personal data



# GDPR compliant data-transfer

Same protection level

Consent (Art. 49)



# GDPR compliant data-transfer

## Same protection level

- Adequacy decision (Art. 45 III)
- Appropriate safeguards (Art. 46)
  - Binding Corporate Rules (BCR) (Art. 46 I, 47)
  - Standard Data Protection Clauses of the Commission (Art. 46 II c)
  - Standard Data Protection Clauses adopted by a supervisory authority (Art. 46 II d)
  - Individual Contractual Clauses, approved by a supervisory authority (Art. 46 III a)
- Enforceable
- “Standard Data Protection Clauses” have been known as “Standard Contractual Clauses (SCCs)” before



[www.your-trips.de/travelmap.php](http://www.your-trips.de/travelmap.php)

# GDPR compliant data-transfer

## Consent (Art. 49)

- Exemption!
  - Section-Title “Derogations for specific situations”
  - Introduction “If not based on Art. 45, 46, 47, ...”

- To be given explicit
- To be given knowing the risks

At the moment, within the USA your personal data is not protected in an extend as it is according to European law. Especially it cannot be guaranteed, that a comparable control for collecting, processing and use of the data by independent authorities or courts occurs or that you can enforce it at a court.

(Example given by EC LÄKH Frankfurt/Main, Germany)

# GDPR compliant data-transfer

## Personal data involved

- Patient data
- CVs of employees  
(CVs of study site staff, CRO-employees)
- Contact data of clinical field specialists

## Advantages

- Only to be done once
- Approved by Data Protection Authority (DPA)

## Disadvantages

- Need to be publicly available
- Company has to comply with

### e.g. Binding Corporate Rules:

# Different roles

## **Data Protection Officer (DPO)** (Art. 37 - 39 GDPR)

A person to give advise to the controller/processor

- on data protection impact assessment (DPIA)
- monitoring DPIA's performance
- on obligations pursuant to e.g. GDPR
- on monitoring compliance to e.g. GDPR and with policies of the company
- on assignment of responsibilities, awareness-raising and training of staff and the related audits;

## **Data Representative**

(Art. 27 in conjunction with Art 3 II GDPR)

A point of contact of a non-Union controller or processor in the Union for data subjects and authorities

# Different roles

## Data Protection Officer (DPO) (Art. 37 - 39 GDPR)

### Obligatory?

- Specified by law when it's a „Must“
- Can be designated voluntarily in other cases

## Data Representative

(Art. 27 in conjunction with Art 3 II GDPR)

### Obligatory?

- YES, for non-Union-based controllers or processors (e.g. sponsors) subject to the GDPR as per Article 3(2) GDPR



# Summary

Transfer of personal data outside of the EU has to be GDPR compliant.

A data protection officer gives advice to the company he/she works for.

A data representative is the Union-based go to person in case of GDPR related issues.

# Sponsor compliance for non-EU companies

Nico Busch, Ass. Jur.

genae