



# REGULATORY UPDATE FROM BOTH SIDES OF THE POND

November 7<sup>th</sup>, 2019

# AGENDA

---

**8:00 a.m. – 8:30 a.m.**

**Registration** – *Breakfast provided.*

**8:30 a.m. – 9:30 a.m.**

**General Data Protection Regulation (GDPR).**

Topics include: controller/processor concept, subject access requests, data breaches, international data transfers, clinical trials, enforcement trends.

*Speaker: [Oliver Süme, Partner, Technology, Outsourcing and Privacy, Fieldfisher](#)*

**9:30 a.m. – 10:15 a.m.**

**EU Medical Device Regulation (MDR).**

Topics include: New obligations, responsible person(s), notified body concerns, MDD vs. MDR.

*Speakers: [Dr. Cord Willhöft, LL.M., Partner, Life Sciences, Fieldfisher](#)*

*and [Jim Murray, M.Sc., Consultant, Gardner Law](#)*

**10:15 a.m. – 10:30 a.m. - Break**

# AGENDA

---

**10:30 a.m. – 11:00 a.m.**

**EU Health Care Compliance.**

Topics include: MedTech Europe Code of Ethical Business Practice, health care compliance in the EU and Germany, transparency.

*Speaker:* [Dr. Cord Willhöft, LL.M., Partner, Life Sciences, Fieldfisher](#)

**11:00 a.m. – 12:00 p.m.**

**US Health Care Compliance.**

Topics include: 2020 AdvaMed revisions, transparency reporting changes, compliance program auditing and monitoring, recent cases.

*Speakers:* [Mark Gardner, M.B.A., J.D., President, Gardner Law](#)

and [Amanda Johnston, J.D., R.A.C., Sr. Attorney, Gardner Law](#)

**12:00 p.m. – 1:00 p.m.**

**Panel Discussion – Lunch provided.**

Speakers from the morning convene for a moderated panel discussion with audience participation.

Come equipped with your questions.

*Moderated by* [Heather Potter, J.D., Associate Attorney, Gardner Law](#)



fieldfisher

## General Data Protection Regulation (GDPR)

Minneapolis, Nov 7

Oliver Süme



## Core concepts

### What is it all about?

- **Territorial scope: Applies to any processor or controller which is**
  - > established in the EU
  - > offers goods and services to data subjects in the EU
  - > monitors the behaviour of individuals in the EU
- **Broad definition of personal data!**



## Core concepts

### Special categories of personal data

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- **genetic data**
- biometric data for the purpose of uniquely identification
- **health**
- sex life or sexual orientation



## Core concepts

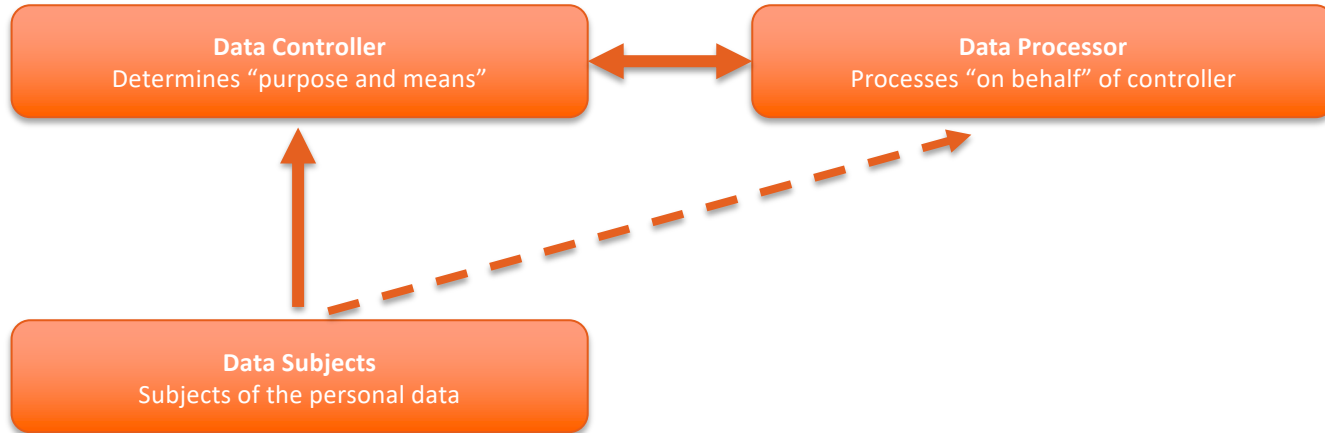
### Lawful processing grounds – Consent based vs. Non-consent-based

#### No hierarchy – all equal and alternative grounds:

- Consent
- Contractual necessity
- Legal obligation (under EU / MS law)
- Vital interests
- Public interests (under EU / MS law)
- Legitimate interests (unless public authority)

# Core Concepts

## Controller vs Processor vs Data Subject







## Core concepts

### Data Subject Rights

- Right to transparency
- Right of access
- Right to rectification
- Right to erasure (aka the right to be forgotten)
- Right to restriction
- Right to portability
- Right to object
- Right not to be subject to automated decision-making



## Core concepts

### Transparency

- Concise, transparent, intelligible
- Easily accessible
- Clear and plain language
- Given in writing

- identity and contact details
- DPO contact details
- purpose of processing and legal basis
- *categories of personal data concerned (Art 14 only)*
- *source of personal data (Art 14 only)*
- recipients or categories of recipients
- global data transfers and legal solutions
- data retention period
- data subject rights
- legitimate interests pursued (if any)
- withdrawal of consent
- right to complain to a DPA



# Coren Concepts

## Data Processing Records

Controller Records	Processor Records
Name and contact details (and joint controller, representative and DPO)	Name and contact details (and joint controller, representative and DPO)
Purpose of processing	Name and contact details of each controller on whose behalf processing data
Categories of data subjects	Categories of processing performed for each controller
Categories of personal data	Details of international transfers (including appropriate safeguards)
Categories of recipients	General description of the technical and organisational security measures
Details of international transfers (including appropriate safeguards)	
Envisaged time limits for erasure (where possible)	
General description of the technical and organisational security measures	

# Enforcement trends









## Enforcement and fines

 POLAND	Polish National Personal Data Protection Office (UODO)	2019-09-10	644,780	Morele.net	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security
 BULGARIA	Data Protection Commission of Bulgaria (KZLD)	2019-08-28	511,000	DSK Bank	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security
 THE NETHERLANDS	Dutch Supervisory Authority for Data Protection (AP)	2019-06-18	460,000	Haga Hospital	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security

## Enforcement and fines

 DENMARK	Danish Data Protection Authority (Datatilsynet)	2019-06-03	200,850	IDdesign A / S	Art. 5 (1) e) GDPR, Art. 5 (2) GDPR	Non-compliance with general data processing principles
 GREECE	Hellenic Data Protection Authority (HDPA)	2019-10-07	200,000	Telecommunication Service Provider	Art. 5 (1) c) GDPR, Art. 25 GDPR	Non-compliance with general data processing principles
 GREECE	Hellenic Data Protection Authority (HDPA)	2019-10-07	200,000	Telecommunication Service Provider	Art. 21 (3) GDPR, Art. 25 GDPR	Non-compliance with general data processing principles
 GERMANY	Data Protection Authority of Berlin	2019-09-19	195,407	Delivery Hero	Art. 15 GDPR, Art. 17 GDPR, Art. 21 GDPR	Insufficient fulfilment of data subjects rights



# The German approach to calculate fines – role model for Europe?

## Global revenue remains key aspect

- The German authorities are of the opinion that  
*“in a modern corporate sanction law with considerable maximum fines, the turnover of a company is a suitable, appropriate and fair link to ensure effectiveness, proportionality and the ability of the company to meet its obligations.”*
- Based on this, the German authorities have developed a five step approach to calculate fines.
- **14.5 Mio EUR** fines have been imposed on a Berlin based real estate company only on Nov 5.



# The German approach to calculate fines – role model for Europe?

## Five step approach:

- Size range based on annual turnover in two steps (Companies with more than 500 Mio EUR turnover only one step)
- Determination of the basic economic value: Annual turnover : 360 (e.g. annual turnover 600 Mio EUR leads to economic value of 1,66 Mio EUR.)
- Classification of the degree of severity of the act in easy, medium, heavy or very heavy (e.g. medium formal infringement means factor 2 – 4, whereas material infringement means 4 - 8).
- Adjustment of the basic economic value on the basis of all other positive and negative factors.



# Processors, controllers and joint controllers





## C2C, C2P and joint controllers

### Controller to Controller

- Data controller determines the purposes and means of the processing and is in charge of the particular processing activity.
- Any data controller pursues own purposes with respect to the processing activities and decides on the specifications of the processing.
- Different to a joint controllership, C2C has not to be defined in a separate controllership agreement. However, C2C constellations have to be transparent to the data subject. The controllers' respective purposes and means of processing must be communicated to the data subject. Any controller has a responsibility to inform data subject on the details of the processing (through a Privacy Statement) and has to respond to the requests for exercising the data subjects' rights.
- **Sponsor and clinical trial site as C2C?**



## C2C, C2P and joint controllers

### Controller to Processor

- C2P relationship implies commissioned processing, i.e. a hierarchical order. Purposes and means of the processing are determined by the controller. However, the processor carries out the actual processing activity for the controller, i.e. there is a certain command structure.
- A data processing agreement (DPA) has to be concluded. Contract can be set up either controller-friendly or processor-friendly.
- Key negotiation issues: Liability and audit rights
- **Payroll provider of operator of external data base to analyze patient data**




## C2C, C2P and joint controllers

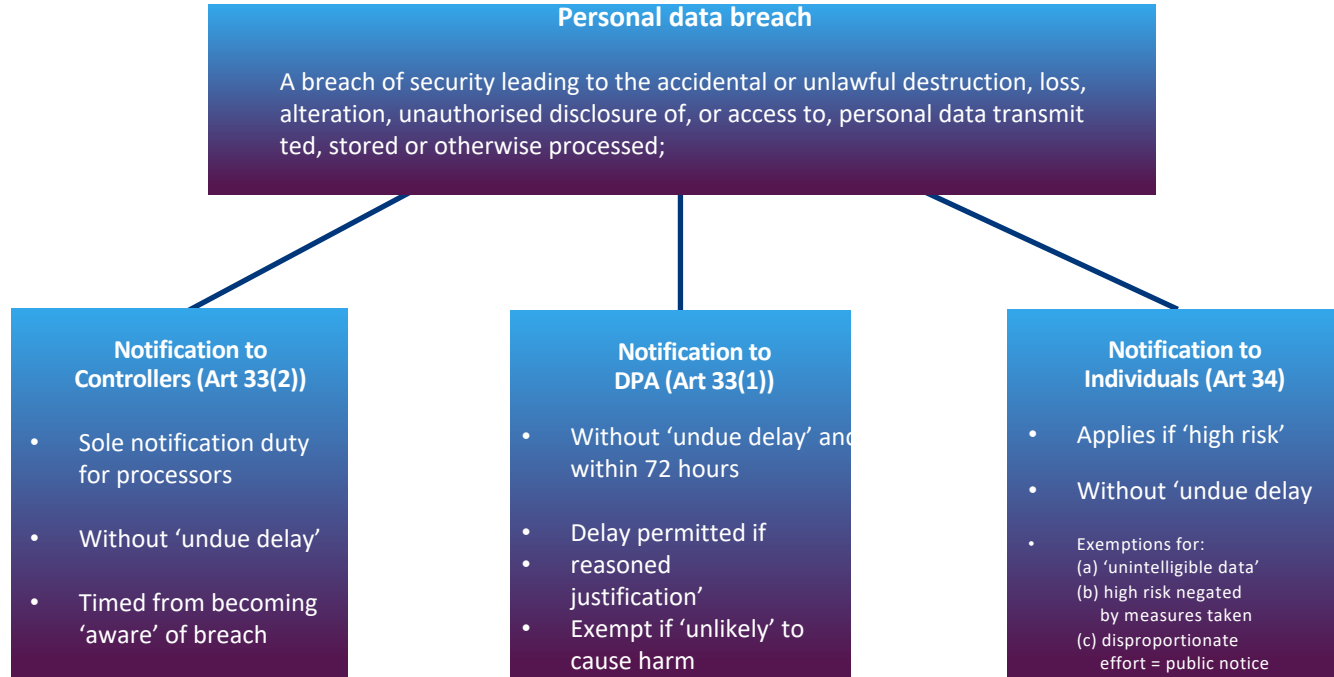
### Joint controllership

- More than one controller is determining the purposes and means of processing.
- Generally, joint controllers take any decisions concerning data processing jointly, not necessarily together. The controllers may either have a joint purpose or different purposes which they jointly pursue.
- Joint controllers need to conclude an arrangement reflecting the respective roles and relationships of the joint controllers vis-à-vis the data subjects.
- Further, they have to make the "essence of the agreement" available: Relevant entities, their registered offices or subs, the purposes which are pursued by each of the controllers, jurisdiction and which of the controllers is responsible for the fulfilment of information obligations.
- **Clinical trials?**

# Data breach notifications

- 
- Blood cholesterol test
  - Blood pressure check
  - Body skin exam
  - Glaucoma test
  - Thyroid hormone test
  - Endoscopy
  - Fasting plasma glucose
- The tablet screen features a dark blue background with various medical icons: a brain in the top right, a world map in the bottom left, and a heart rate monitor waveform in the bottom right. A central checklist is displayed with a plus sign icon to its left. The text 'Health Care Enrollment Period' is visible in the middle left area of the screen.

# Data breach notification





# Data breach notifications

## Numbers

- Around 100.000 data breach notifications across Europe since May 2018 (estimated)
- Reporting of data breaches when health data is concerned
- Ranking:
  1. Misdirected letters / orders
  2. Hacking and malware
  3. Misdirected emails
  4. Theft of data media



# Data breach notifications

## Lessons learned

- Well implemented processes are key to meet GDPR requirements
- Providing information in phases has proven to be effective and well accepted
- Minor breaches often receive no feedback from authorities at all
- Better safe than sorry?



# Thank you for your attention



**Oliver Süme**  
Partner

Fieldfisher (Germany) LLP  
Am Sandtorkai 68  
20457 Hamburg  
Germany

+49 40 8788698 217  
oliver.sueme@fieldfisher.com  
www.fieldfisher.com

