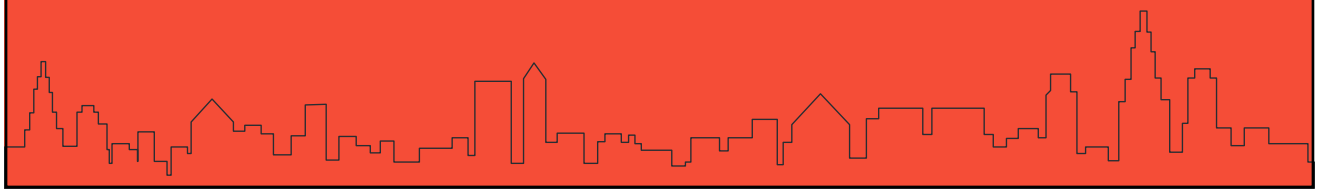
Impacts of GDPR on CDISC ?

Xavier Gobert

GUF CDISC Paris
23 Mars 2017



Introduction

Consistent protection of consumer and personal data across EU nations

What is GDPR ?

GDPR = General Data Protection Regulation

EU regulation, not a directive

Local regulations will be superseded by the new legislation

It introduces tougher fines for non-compliance and breaches, and gives people more to say over what companies can do with their data

Agreed upon by the European Parliament and Council in April 2016 / becomes effective on May 25, 2018

3

Introduction

Consistent protection of consumer and personal data across EU nations

Objectives

3 drivers for EU

1. give people more control over how their personal data is used. To address issues and challenges of the internet and cloud technology GDPR tends to improve trust in the emerging digital economy.
2. give businesses a simpler, clearer legal environment data protection law identical throughout the single market.
3. fight Cyber Criminality

Scope

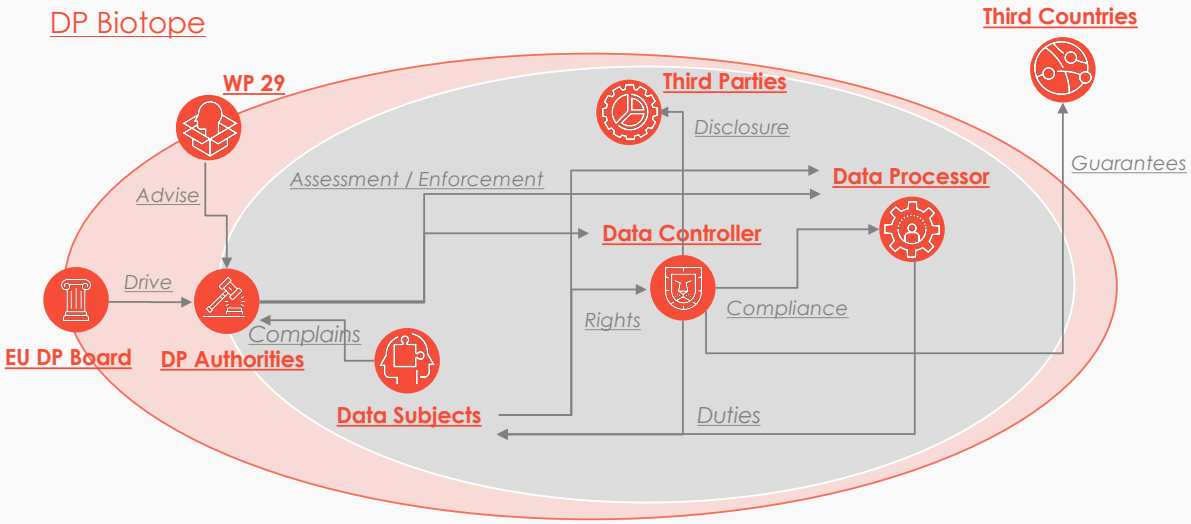
Any company that markets goods or services to EU residents, regardless of its location, processing personal data is subject to the regulation **> GLOBAL IMPACT**

4

Introduction

Consistent protection of consumer and personal data across EU nations

DP Biotope



Introduction

... a major step towards a Digital Single Market

5

Motivations

- Digital Economy : "*DATA IN THE 21st Century is like Oil in the 18th Century: an immensely, untapped valuable asset. Like oil, for those who see Data's fundamental value and learn to extract and use it there will be huge rewards.*"
- Cyber Crime = the greatest threat to every company
  - Cost of breaches estimated to
    - 2013 : 100 b$
    - 2015 : 400 b$
    - 2019 : 2,100 b$

Introduction

... a major step towards a Digital Single Market

6

The price of personal data (online platforms)

If you are not paying for something, it should be known that you are the product.

Data has become a strategic asset that allows companies to acquire or maintain a competitive edge.

- Facebook decided to acquire WhatsApp for $19 billion; that is, to pay $30 for each of its 600 million users.
- Similarly, it also paid $30 for each of the 33 million Instagram users back in 2012.
- Similar computation when Minecraft was acquired by Microsoft.
- Between 15$ and 40$

7

Introduction

… a major step towards a Digital Single Market

The price of personal data (data brokers)

Data brokers make money by selling this data compiled in comprehensive lists or databases to marketers and non-profits.

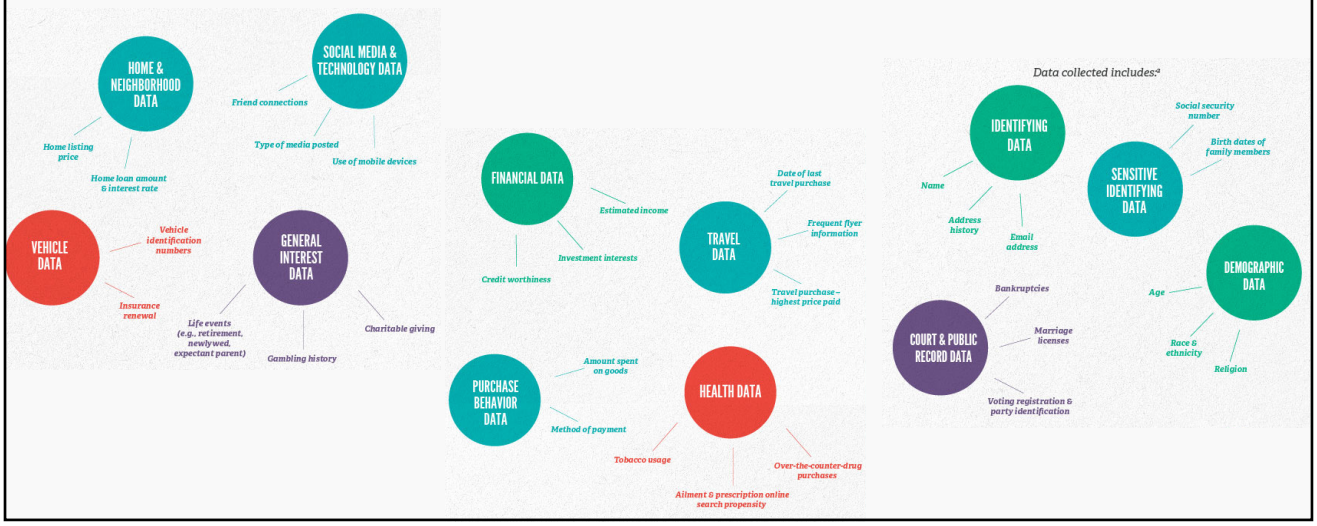
- Google and Facebook dominate the digital advertising market by using your data to allow marketers better targeting options.
- Loyalty cards
- Data from your mobile phones

- file:///Users/xaviergobert/Downloads/facebook-100009134386549/html/friends.htm
- https://www.google.com/maps/timeline?pb=!1m2!1m1!1s2016-11-18
- http://www.ft.com/cms/s/2/927ca86e-d29b-11e2-88ed-00144feab7de.html?ft_site=falcon#axzz4bfPG6Ww5

8

Introduction

… a major step towards a Digital Single Market



Introduction

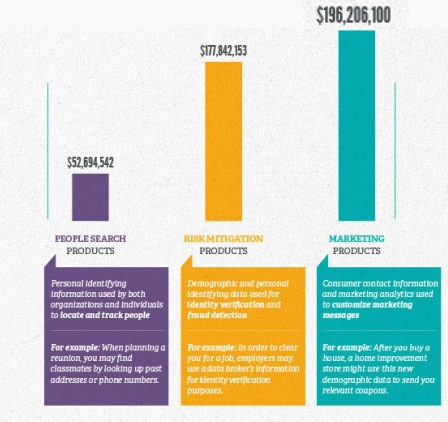
... a major step towards a Digital Single Market

9

A study of **nine key brokers** found that they generated approximately

$426 MILLION

in revenue by selling customer data via marketing, risk mitigation and people search products in 2012.[11]



http://www.visualcapitalist.com/much-personal-data-worth/

Introduction

... a major step towards a Digital Single Market

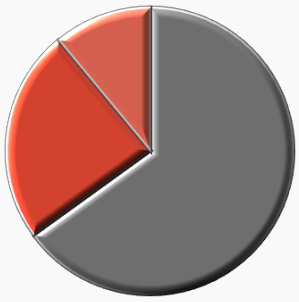
10

Cybercrime <> Cybersecurity

Cybersecurity refers to preventative methods (technical, organizational and legal) used to protect information from being stolen, compromised or attacked.

Who are the Cybercriminals ?

- Criminal Organizations
- States
- Cyberterrorists
- Cyberactivists (anonymous, white hat)



Christophe AUBERGER
Director Systems Engineering – Fortinet
Membre du clusif – Membre du groupe de travail SCADA

11

Introduction

… a major step towards a Digital Single Market

Example : TV5 Monde

12

Introduction

… a major step towards a Digital Single Market

Example : Jeep Cherokee

13

Introduction

... a major step towards a Digital Single Market

Example : Smart TV - Samsung

In 2015, there was a mini furore about Samsung sharing the conversations recorded by the TV with third parties.

FBI had successfully searched the Samsung TV of a suspect as part of an investigation into child sexual abuse material.

CIA was developping TV malware Weeping Angel

14

Introduction

... a major step towards a Digital Single Market

The question is not « Why ? »

It's « When ? » and « Since when ? »

https://threatmap.fortiguard.com/

https://cybermap.kaspersky.com/

15

Introduction

... a major step towards a Digital Single Market

GDPR Content

1. Data processing principles : fairly and lawfully, transparent and minimized, …
3. Data Subjects rights : to be forgotten, corrected, access to data and portability
   - ❖ Data Controllers Responsibilities: DPOs, reporting to DPAs, vendors validation, data breaches reporting
   - ❖ Data Processors : DPOs, reporting to DPAs, use of sub-contractors, …
   - ❖ Privacy by design and by default
2. Data Transfers
   - ❖ Fines and Penalties : 10 M€/20 M€ or 2%/4% of Global revenues

16

Presentation Content

1. Introduction
2. SDTM Vs GDPR
3. Data Transfers
4. Data Portability
5. Use Cases
6. Conclusions

Data Processing Principles

… "The value of an idea lies in the using of it", Thomas A. Edison, American Inventor

Data Processing Principles

The value of an idea lies in the using of it

GDPR applies to the processing of **personal data** wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

- ❖ technologically neutral and not depend on the techniques used.
- ❖ apply to the processing of personal data by automated means, as well as to manual processing, if the personal data are contained or are intended to be contained in a filing system.
- ⛔ Files which are not structured according to specific criteria should not fall within the scope of GDPR.
- ⛔ Not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity.

19

Data Processing Principles

The value of an idea lies in the using of it

Personal Data means 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.

- Identifier can be a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- Apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data
- Apply to any information concerning an identified or identifiable natural person.
- Not cover the processing of personal data which concerns legal persons.

20

Data Processing Principles

The value of an idea lies in the using of it

Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information.

- Provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
- Pseudonymisation of personal data can reduce the risks to the data subjects concerned.
- Pseudonymisation is not intended to preclude any other measures of data protection.

Data Processing Principles

21

The value of an idea lies in the using of it

On the concept of personal data:

- Pseudonymisation is the process of disguising identities. The aim of such a process is to be able to collect additional data relating to the same individual without having to know his identity.
- Pseudonymisation can be done in a retraceable way by using correspondence lists for identities and their pseudonyms.
- Pseudonymised data are retraceable. Using a pseudonym means that it is possible to backtrack to the individual, so that the individual's identity can be discovered, but then only under predefined circumstances.
- In that case, data protection rules apply. The risks at stake for the individuals with regard to the processing of such indirectly identifiable information will be mitigated.

Data Processing Principles

22

The value of an idea lies in the using of it

GDPR

Distinguish 3 types of privacy grading

- Grading 3: situations where directly identifiable personal data are needed due to the nature of the research/the processing.

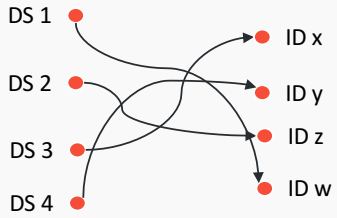
  Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols (e.g internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags). When combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.

Data Processing Principles

The value of an idea lies in the using of it

GDPR

- Grading 2: indirectly identifiable personal data: lower level of aggregation, partial anonymization, pseudonymisation or key-coded data.



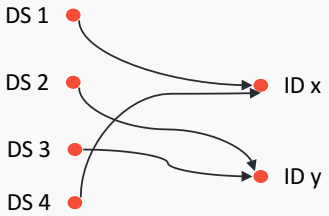
Data Processing Principles

The value of an idea lies in the using of it

~~GDPR~~

- Grading 1: unidentifiable personal data: data are anonymised or aggregated in such a way that there is no remaining possibility to (reasonably) identify the data subjects.

  Use of hashing algorithms (MD5), mathematical functions (Modulo), …



Data Processing Principles

The value of an idea lies in the using of it

For a Data Privacy Grade 2 :

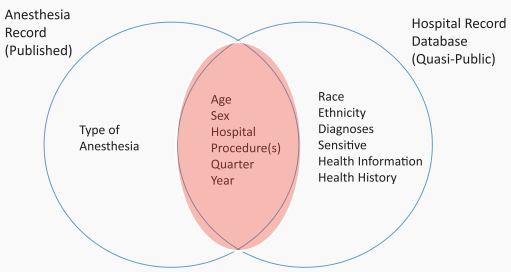
- Reinforce the security of the decoding key
  - Management of the patient id
  - Minimization of identifying information (e.g. sample code, ip)
- Be careful with the publishing of results
  - Avoid small pooling of results
  - Be careful with data transfers to third parties
- Follow regulations for data transfers to third countries

Data Processing Principles

The value of an idea lies in the using of it

« The Risks to Patient Privacy from Publishing Data from Clinical Anaesthesia Studies » , Liam O'Neill, PhD,* Franklin Dexter, MD, PhD,† and Nan Zhang, PhD , Jun 2016

- Privacy implications of posting data from small, randomized trials, observational studies, or case series in anaesthesia from a few (e.g., 1–3) centers involving 4 to 40 patients per group. Examples of such studies would include 40 patients randomized into 2 groups for a pharmacokinetic analysis; 40 patients in a registry with malignant hyperthermia or 40 patients having magnetic resonance imaging under general anaesthesia at night.



27

Data Processing Principles

The value of an idea lies in the using of it

« The Risks to Patient Privacy from Publishing Data from Clinical Anaesthesia Studies » , Liam O'Neill, PhD,* Franklin Dexter, MD, PhD,† and Nan Zhang, PhD , Jun 2016

- the Texas Inpatient Public Use Data File for 2013 from the Texas Department of State Health Services. The database includes >2.8 million records (rows) and 255 distinct attributes (columns), including up to 24 procedure codes.

Combination of attributes	Unique records	Valid records*	Percent unique	Percent of patients	Number of elements conjoined
Hospital, gender, quarter, primary procedure	79,989	491,036	16.3	59	4
Hospital, gender, quarter, 2 procedures	71,006	110,309	64.4	13	5
Hospital, gender, quarter, 3 procedures	55,278	67,223	82.2	8	6
Hospital, gender, quarter, 4 procedures	39,455	44,180	89.3	5	7
Hospital, gender, quarter, 5 procedures	31,137	33,804	92.1	4	8
Hospital, gender, quarter, 6 procedures	24,411	30,377	80.4	4	9
Hospital, gender, quarter, 7 procedures	17,936	19,282	93.0	2	10
Hospital, gender, quarter, 8 procedures	11,177	11,341	98.6	1	11
9 or more procedures	N/A	29,371	N/A	4	N/A
Total		836,923		100	

28

Data Processing Principles

The value of an idea lies in the using of it

Real Case: Netflix

- Netflix maintains a database of movie ratings made by their customers.
- In 2006, Netflix published part of this database and offered a prize of one million dollars to anyone who could develop a better algorithm to predict customer movie ratings.
- In 2007, 2 computer scientists from the University of Texas at Austin announced that they had re-identified 2 individuals from the Netflix database by linking it to a public database of movie ratings and therefore knew all of the movies that they had rated. The researchers showed that an adversary needed to know only 6 (out of 8) movie ratings to find exact matches for 99% of the population. Moreover, the adversary could find exact matches for 42% of the population with as few as 2 movie ratings.
- As a result of this successful re-identification, Netflix faced a class action lawsuit for violating its privacy policy, which it settled for an undisclosed amount.

29

Data Processing Principles

The value of an idea lies in the using of it

GDPR

Regarding SDTM/AdaM

1. Demo (DM) :
   - USUBJID
   - INVNAM
   - AGE
   - SEX
   - RACE
   - ETHNIC
   - COUNTRY
   - xxSTDTC
2. Trial Disease Milestones (TM) :
   - MIDSTYPE
   - SMSTDTC
3. Events Observations Class
   - --TERM
   - --MODIFY
   - --LLT
   - --ACNOTH
   - --TOX
   - --DTC
4. Events Observations Class
   - --XFN
   - --NAM
5. Findings Observation Class :
   - some tests (like Height, Weight, BMI)
6. Supplemental Qualifiers (SUPP--)

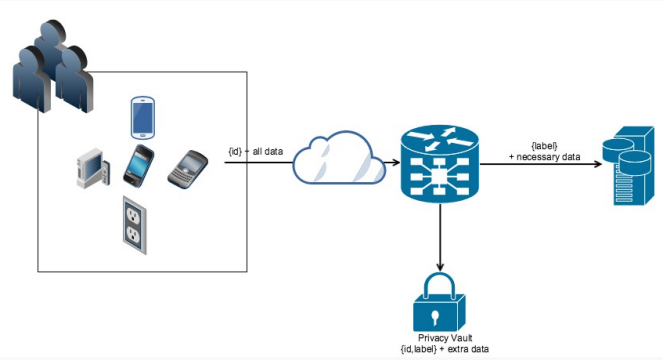
Minimization of information and control a minimal pooling for results publishing

30

Data Processing Principles

The value of an idea lies in the using of it

GDPR



Efficiently manage IDs (Subj ID and IP) and don't record unnecessary information

Data Transfers

… "Data is a precious thing and will last longer than the systems themselves." ,

Tim Berners-Lee, inventor of the World Wide Web

Data Transfers

32

… Data is a precious thing and will last longer than the systems themselves

Main objectives of CDISC : streamline the data flows and facilitate data transfers

- SDTM and AdaM : transfer study data and study results to FDA
- ODM : to archive the data and transfer the data between data collection systems

Main objective of GDPR : control the data transfer (facilitate inside EU but control & limit outside EU)

33

Data Transfers

... Data is a precious thing and will last longer than the systems themselves

The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations.

It's prohibited unless:

- the jurisdiction in which the recipient is located is deemed to provide an adequate level of data protection;
- the data exporter puts in place appropriate safeguards; or
- a derogation or exemption applies.

34

Data Transfers

... Data is a precious thing and will last longer than the systems themselves

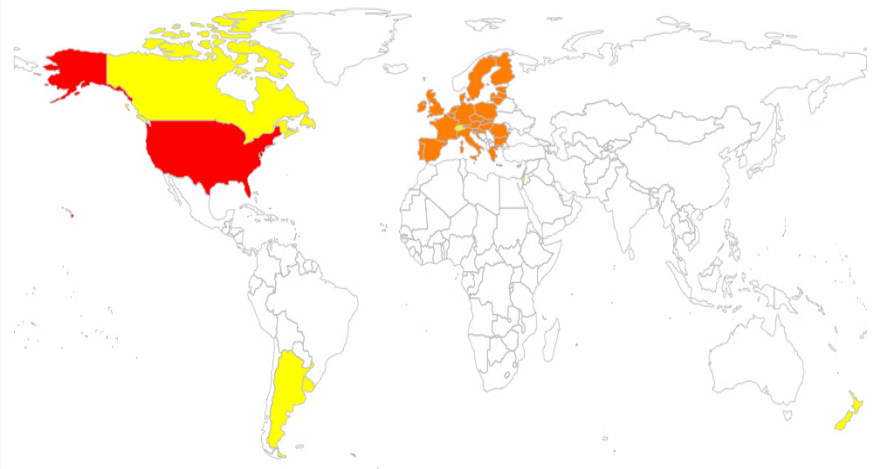
Before transferring data to a third party, check the location

- ✓ OK for EU
- ✓ OK for adequate countries : Andorra, Argentina, Canada (where PIPEDA applies), Switzerland, Faero Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.
- ✓ OK for US if companies decided to comply the Privacy Shield (no more the Safe Harbor)
  - https://www.privacyshield.gov/list

35

Data Transfers

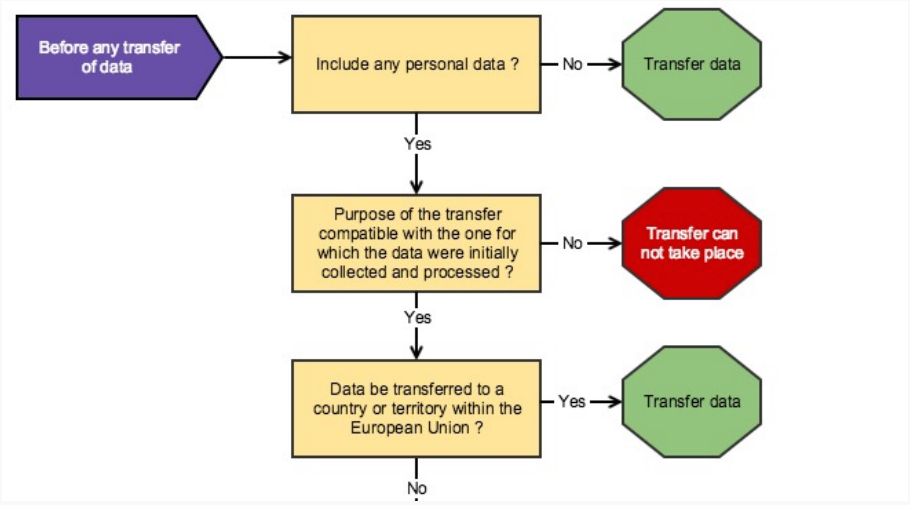
... Data is a precious thing and will last longer than the systems themselves



36

Data Transfers

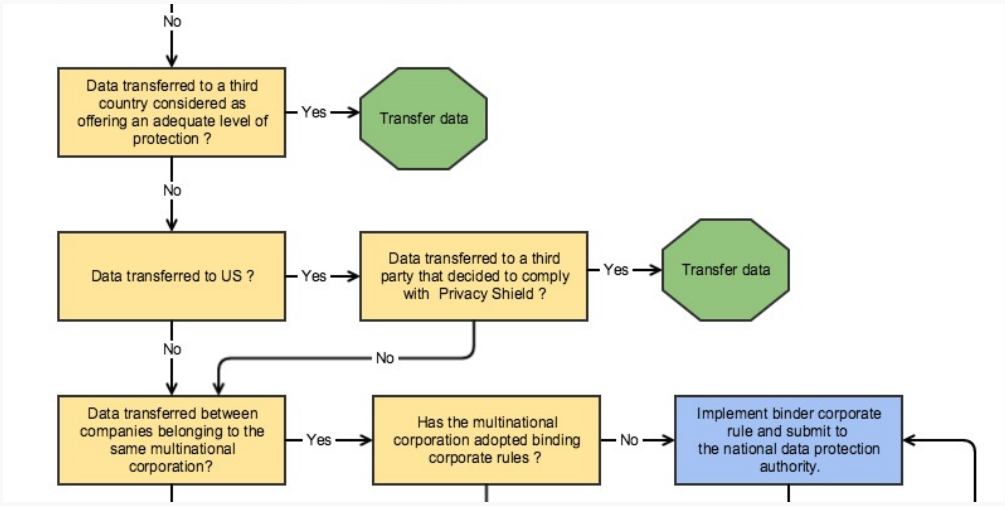
... Data is a precious thing and will last longer than the systems themselves



37

Data Transfers

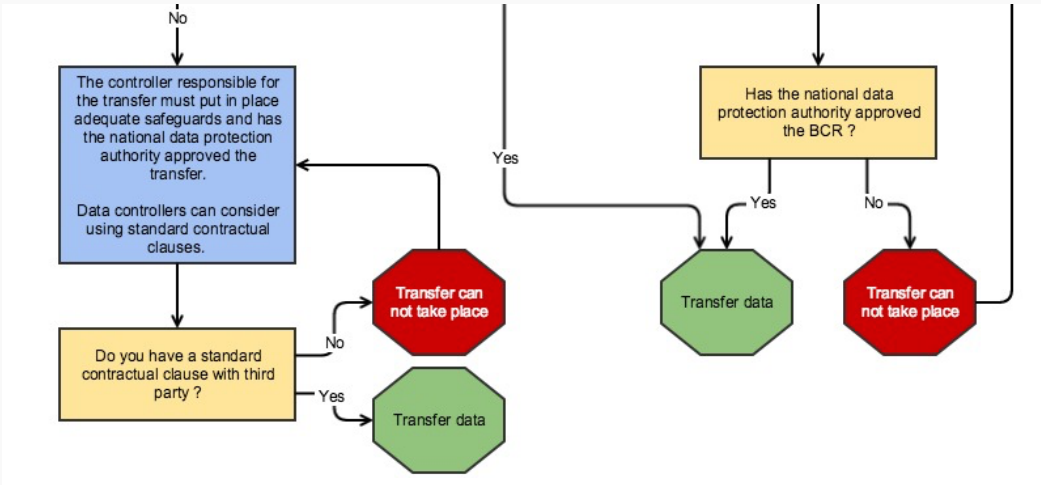
... Data is a precious thing and will last longer than the systems themselves



38

Data Transfers

... Data is a precious thing and will last longer than the systems themselves



39

Data Transfers

… Data is a precious thing and will last longer than the systems themselves

Model of contract

- http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm

List of companies for which the EU BCR cooperation procedure is closed :

- http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm

Privacy shield for pharma & medical products :

- https://www.privacyshield.gov/article?id=14-Pharmaceutical-and-Medical-Products
- Authorized to transfer data to government agencies like the Food and Drug Administration.

Data Portability

… "The more data banks record about each one of us, the less we exist"

– Marshall McLuhan, Canadian philosopher

41

Data Portability

... The more data banks record about each one of us, the less we exist

EU data protection law provides data subjects with a wide array of rights that can be enforced against organisations that process personal data.

These rights may limit the ability of organisations to lawfully process the personal data of data subjects, and in some cases these rights can have a significant impact upon an organisation's business model.

- Right of access
- Right of rectification
- Right to erasure
- Right of data portability

42

Data Portability

... The more data banks record about each one of us, the less we exist

Right of data portability

Data subjects have the right to transfer their personal data between controllers (e.g., to move account details from one online platform to another).

- New obligation (UK Data Privacy Directive : Did not directly address the right of data portability.)
- For some organisations, this new right to transfer personal data between controllers creates a significant additional burden, requiring substantial investment in new systems and processes.
- Can have a sense for patients.

43

Data Portability

… The more data banks record about each one of us, the less we exist

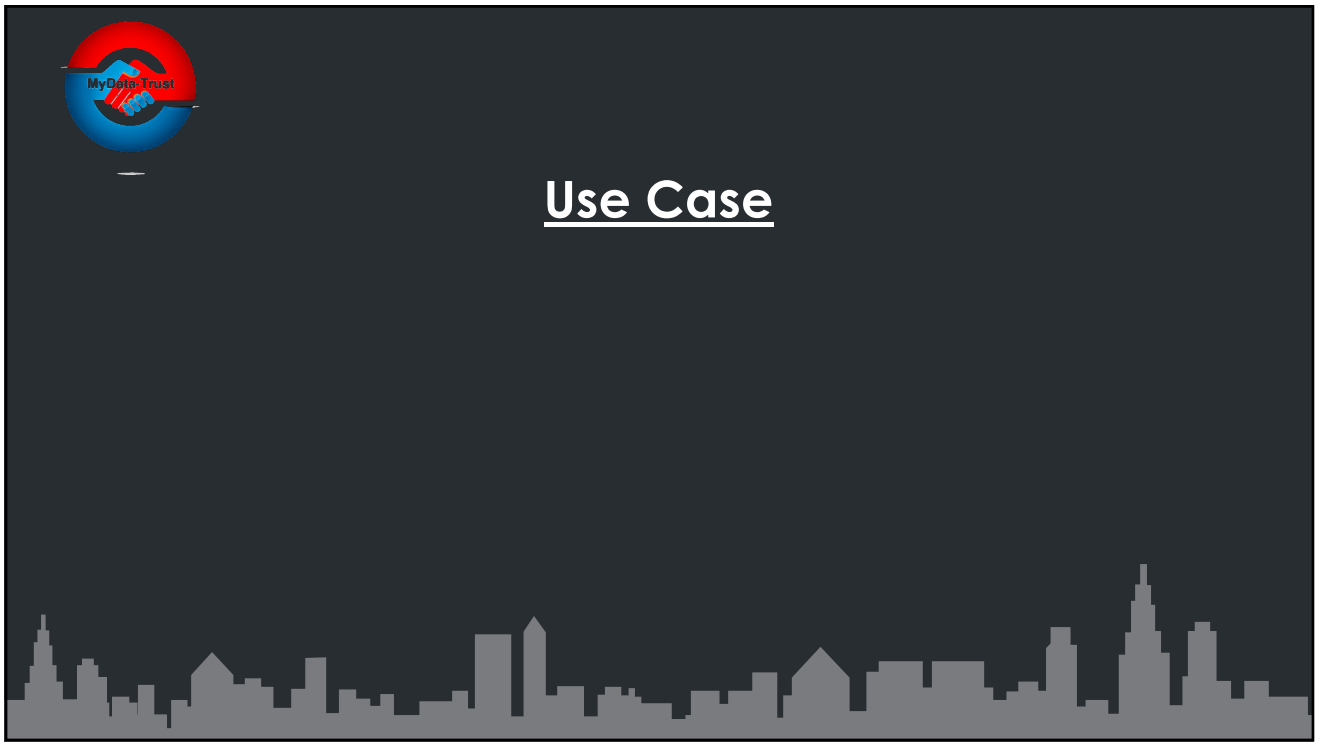
- Data to be ported to them or a new provider in machine readable format
  1) provided by the data subject to the controller (interpreted broadly);
  2) is processed automatically; and
  3) is processed based on consent or fulfilment of a contract.
- The request must be met within one month (with extensions for some cases) and any intention not to comply must be explained to the individual.

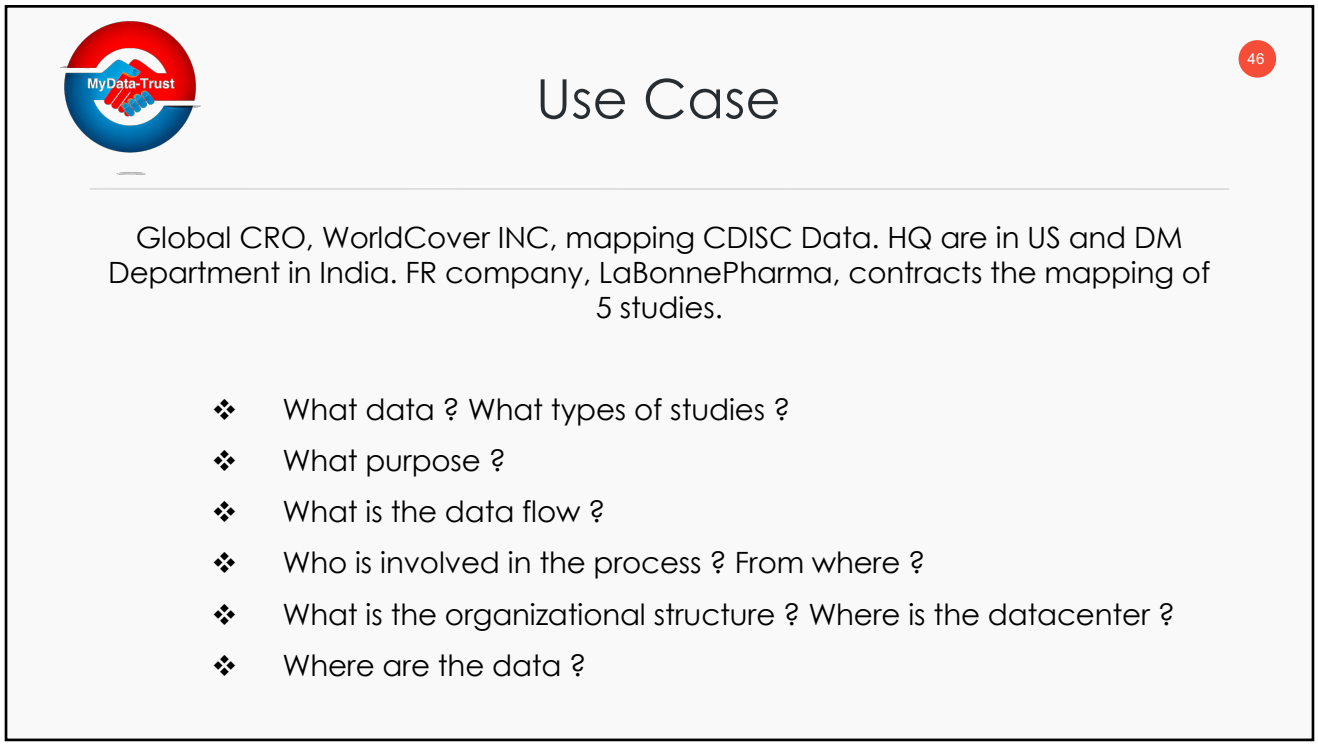
44

Data Portability

… The more data banks record about each one of us, the less we exist

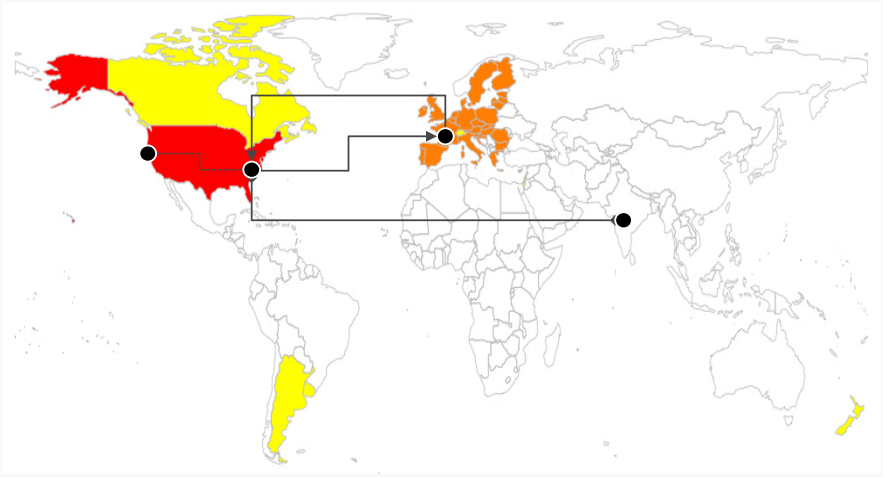
- No specific data transfer format defined !
- Can be good to promote CDISC models like
  1) define.xml
  2) ODM
- CDISC allows to address this new regulation.


MyData-Trust
Use Case


MyData-Trust
46
Use Case
Global CRO, WorldCover INC, mapping CDISC Data. HQ are in US and DM Department in India. FR company, LaBonnePharma, contracts the mapping of 5 studies.
❖ What data ? What types of studies ?
❖ What purpose ?
❖ What is the data flow ?
❖ Who is involved in the process ? From where ?
❖ What is the organizational structure ? Where is the datacenter ?
❖ Where are the data ?

47

Use Case



Conclusions

…"With the new day comes new strength and new thoughts."

Eleanor Roosevelt

49

Conclusions

… …With the new day comes new strength and new thoughts

- Effective Start Date of GDPR : 25 th May 2018
  - No delay to expect
  - Some rooms for national implementation ("GDPR Implementation Act") regarding the rights of data subjects
- From the Start Date
  - Data breaches reporting
  - Fines and penalties operating (e.g. Bayer has no BCR, 2% of TO (47 b€ in 2015) = 940 M€)

50

Conclusions

… …With the new day comes new strength and new thoughts

- Significant additional burden, requiring substantial investment in new systems and processes.
  - ✓ Transparency for patients
- All of us we are impacted !
  - The first will be the CROs
- Impact on CDISC is limited
  - No restriction
  - Additional controls that must be implemented in your processes

Thanks for Your Attention

x.c.gobert@mydata-trust.com
Twitter : @XGOMDT