AXON
science based lawyers

RANKED LEADERS IN THEIR FIELD CHAMBERS EUROPE 2014

LEGAL ASPECTS OF BIG DATA ANALYTICS

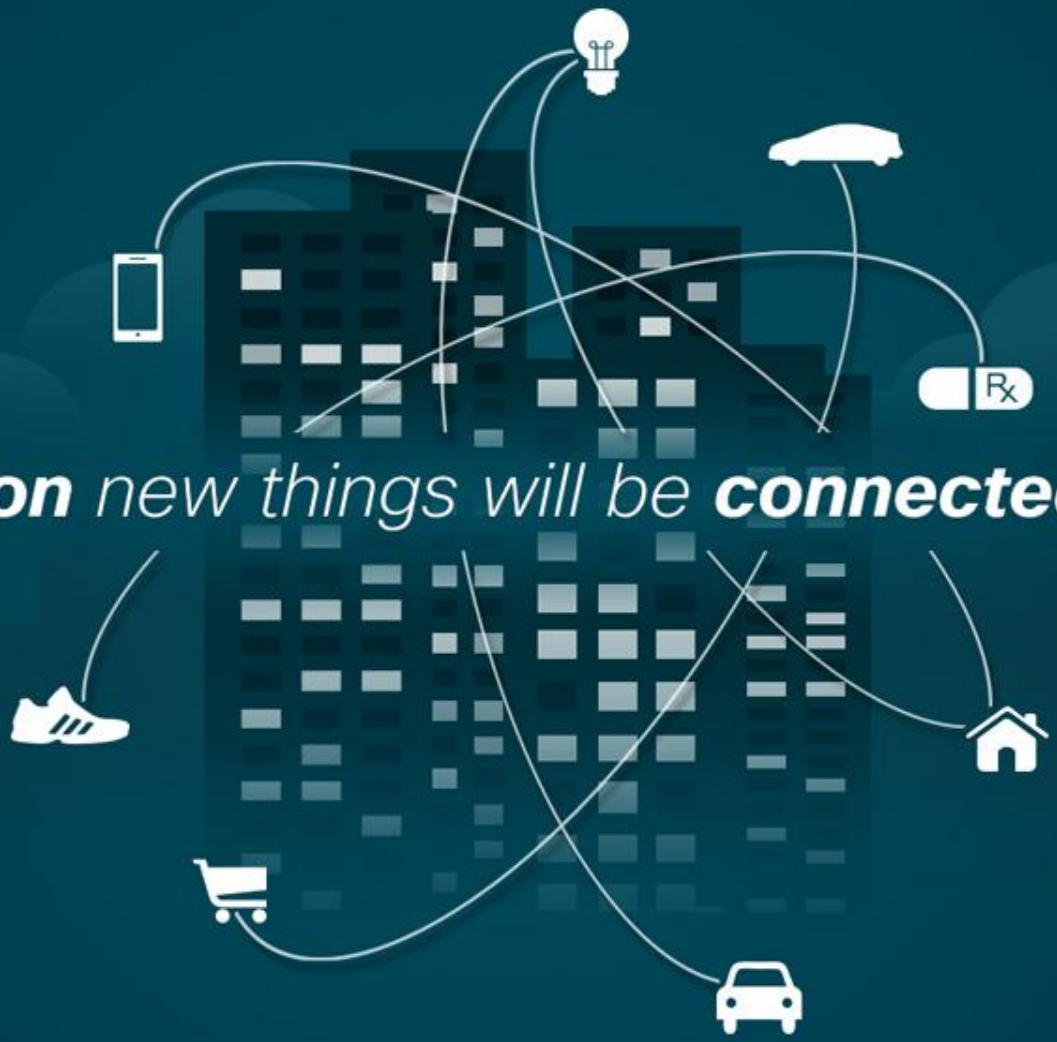
FHI themabijeenkomst 'Wet bescherming persoons- en patiëntgegevens en Big Data'

Erik Vollebregt

health
food
technology

THE INTERNET **OF EVERYTHING** IS HERE.

As the Internet evolves, so will we.

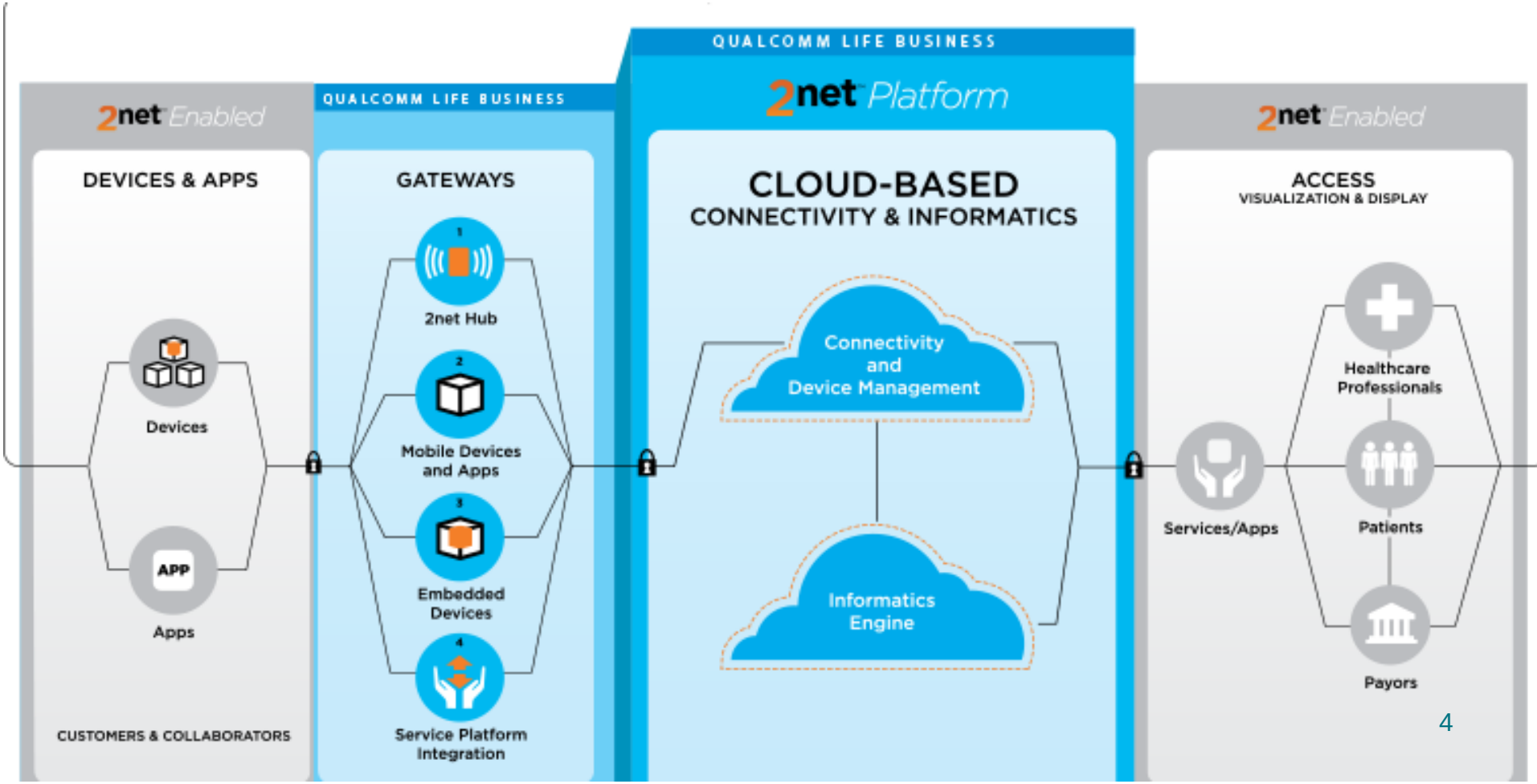


***37 billion** new things will be **connected by 2020**.*

#IoE #TomorrowStartsHere

cisco

Typical big data cloud configuration



Overview

- Definition of Big Data
- Legal perspective of data
- Big Data, Data Protection & Privacy
- Looking forward: the General Data Protection Regulation

Where do we find Big Data?

‘Big Data is everywhere’ – *Financial Times 27 June 2014*

Legal definition of Big Data =

LIKE

FEBRUARY
30TH
(NON-EXISTENT)

What is Big Data?

European Commission 2 July 2014 (COM(2014) 442 final):

“The term “Big Data” refers to large amounts of different types of data produced with high velocity from a high number of various types of sources. Handling today’s highly variable and real-time datasets requires new tools and methods, such as powerful processors, software and algorithms, going beyond traditional “data-mining” tools designed to handle mainly low-variety, small scale and static datasets, often manually.”

EUROPEAN
COMMISSION

Brussels, 2.7.2014
COM(2014) 442 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

Towards a thriving data-driven economy

Big Data - EU

European Commission
25 March 2015:

“Big data is a goldmine, but it also raises important challenges, from ownership to data protection to standards. These need to be addressed to unlock its potential.”

To be able to seize opportunities the Commission aims to make *“sure that the relevant legal framework and policies, such as on interoperability, **data protection**, security and IPR are data-friendly, leading to more regulatory certainty for business and creating consumer trust in data technologies”*

http://europa.eu/rapid/press-release_IP-15-4653_en.htm

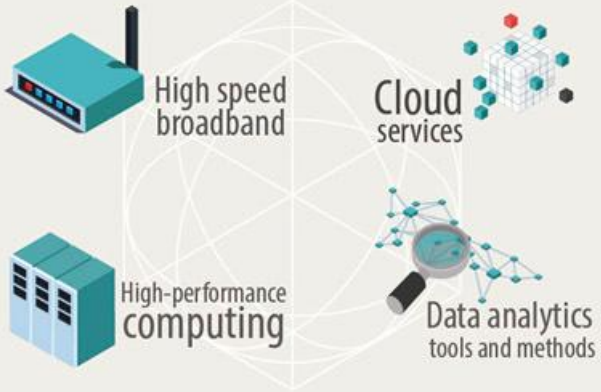
https://ec.europa.eu/digital-agenda/en/

HOW CAN BIG DATA MAKE A DIFFERENCE?

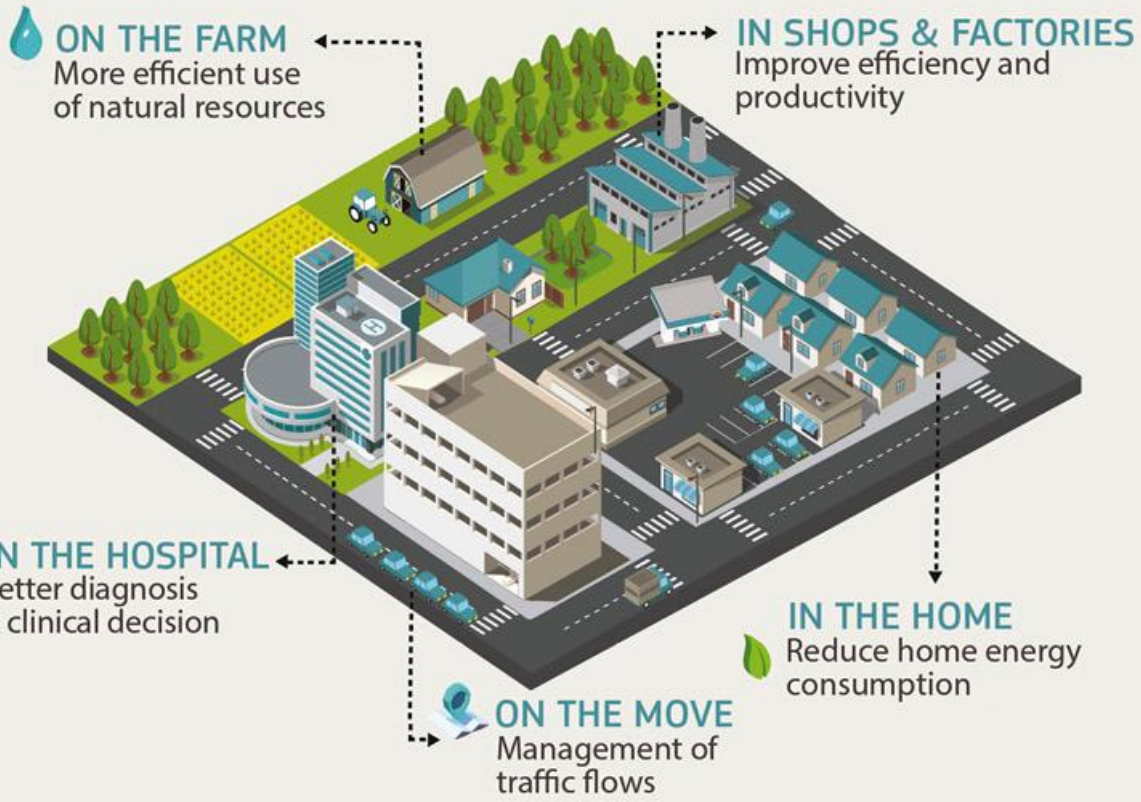
DO YOU KNOW?

Decoding the human genome took

ALL OF THIS IS POSSIBLE BECAUSE OF



REAL LIFE APPLICATIONS



Data will create HUNDREDS OF THOUSANDS of new jobs

e.g. In the UK 240% Big data specialists by 2017 ≈ 69 000 Jobs

& growth € 17 BILLION worldwide in 2015

http://ec.europa.eu/information_society/newsroom/image/infographic_big%20data%20export%20indd_1200px_6288.jpg

Definition of Data in IT

ISO/IEC 2382-1:1993 (Information technology — Vocabulary — Part 1: Fundamental terms)

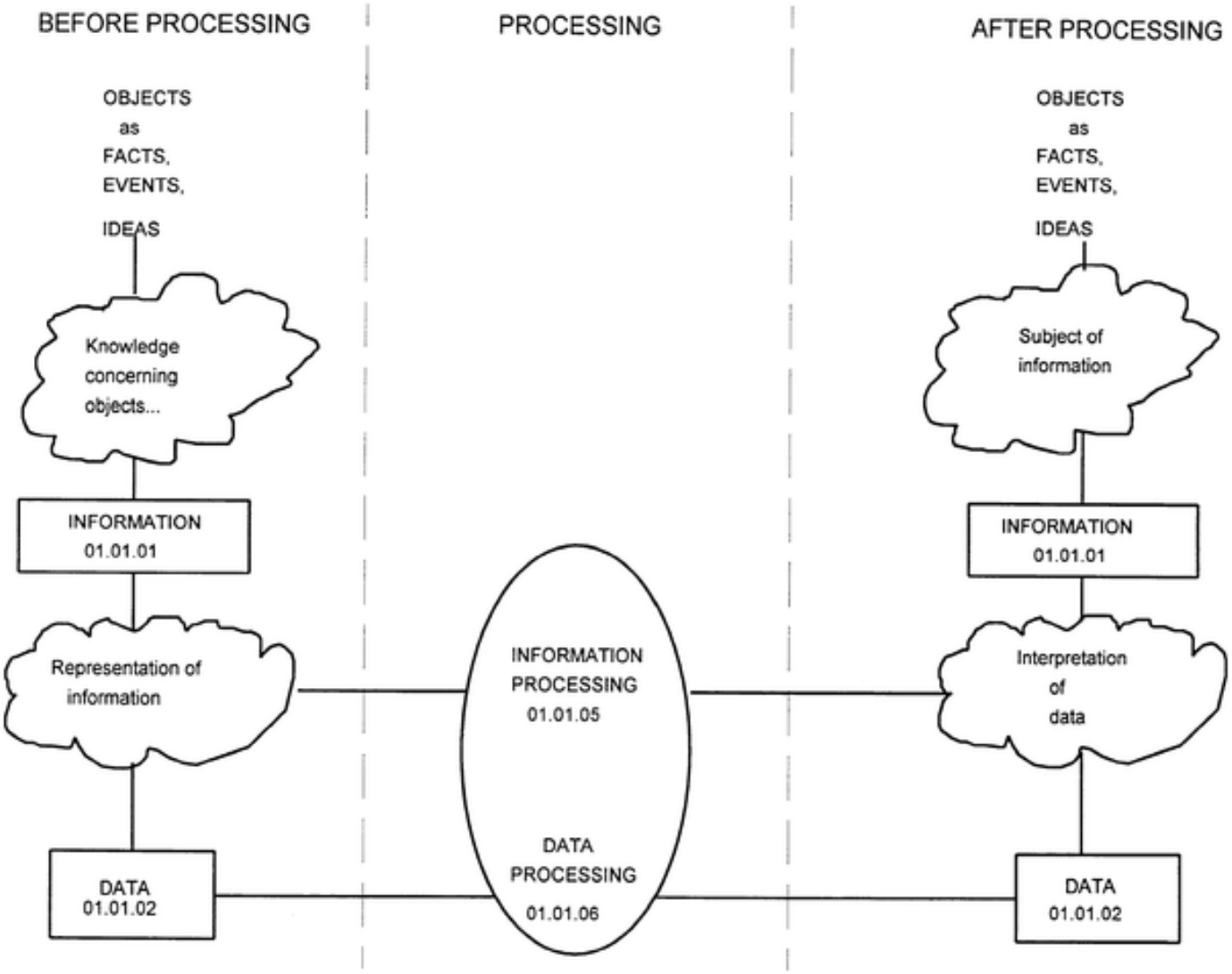
Data
‘A reinterpretable representation of *information* in a formalized manner suitable for communication, interpretation, or processing.
Data can be processed by humans or by *automatic* means.’

Information (in information processing)
‘Knowledge concerning objects, such as facts, events, things, processes, or ideas, including concepts, that within a certain context has a particular meaning.’

https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:-1:ed-3:v1:en

ISO/IEC 2382-1:1993

Figure 1 — Interrelationships between information and data



Legal perspective on data?

- No legal definition of ‘data’
- No rights ***in*** data (no property or ownership concept)
- Rights and obligations ***in relation to*** data

Data law:

- Data regulation (focus on data protection)
- Contracting
- IP rights (copyright, database right)

IP: Copyright

Protects the *original* form or expression of information but not the underlying information itself.

- "original" only if *"selection or arrangement of contents is author's own intellectual creation*".
- Infringement by translation or making an altered version. Successful claim needs to show at least:
    - That copyright exists (pragmatic approach 'what is worth copying is worth protection')
    - Claimant owns the copyright
    - Work is within copyright (life plus 70 years for software and databases)
    - Infringement (substantial part is reproduced without authorisation)

IP: Databases

EU Database rights (Directive 96/9)

- Excludes programs used in making/operating database

Database: "*a collection of independent works*, data or other materials which (a) are arranged in a systematic or methodological way and (b) are individually accessible by electronic or other means*"

- Maker's right where substantial investment (qualitatively/ quantitatively) in making the database.

- Lasts 15 years from initial creation. 'Refreshed' if any substantial change is made.

- Infringed by '*extraction and re-utilisation*' of *substantial* parts *or* repeated and systematic re-utilisation of *in*substantial parts.

Contracting

IP in contracts. Attention should be paid to:

- Scope of rights being licensed
- Use of the data and derived data (and what is permitted in the terms of the provider?)
- Warranties of compliance with regulations
- Liabilities
- Duration and termination of supply and post-term use

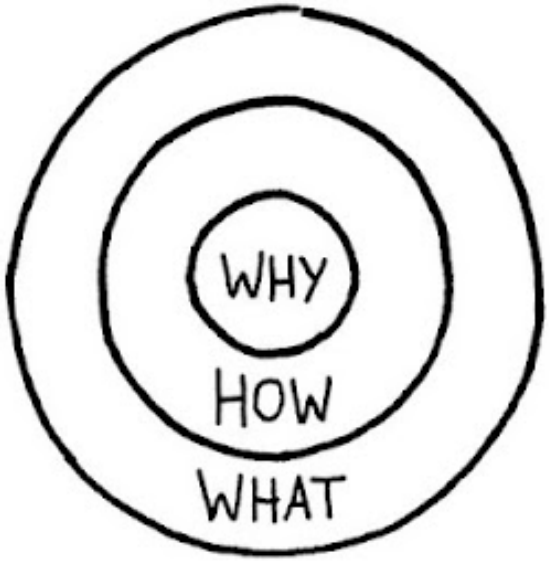
Coming up: Big Data - data protection & privacy

What is privacy?

You want a piece of me?

- **Privacy policy**

Tell people WHY you want their data, tell them HOW you handle the data and WHAT you are going to do with it.



- **Privacy by design**

Make privacy and security part of the development of your products.

Data protection in the EU

European Commission Greenpaper on mHealth: one of the issues “at stake”: data protection, including security

Current legal framework: Data Protection Directive (95/46/EC)
in flux: General Data Protection Regulation proposal

EU approach: fundamental right (Article 8 European Convention on Human Rights) -> emphasis on data subject interests

Brussels, 10.4.2014
COM(2014) 219 final

GREEN PAPER

on mobile Health ("mHealth")

{SWD(2014) 135 final}

Big Data – Data processing?

Definition of 'processing':

'*Any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.*' (Data Protection Directive).

Parties involved in processing

- **Controller:**

‘The natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data’

- **Processor:**

‘A natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller’

- **Third party**

- **Data subject**

- Right to access
- Right to correction
- Right to erasure
- Right to objection

Personal data?

Collecting and processing data may give rise to personal data processing and related obligations.

Personal data: any information relating to an *identified* or *identifiable* natural person ('data subject'); whether directly or indirectly identifiable.

"data relates to an individual if it refers to the identity, characteristics or behaviour of an individual or if such information is used to determine or influence the way in which that person is treated or evaluated" (WP136)

Big Data & Data Protection - issues

Informed consent vs. the principle of purpose limitation

- Consent: "*…any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed*". Special data? *Explicit* consent (see article 29 WP Opinion 15/2011).

Is the new purpose compatible with original purpose? No? -> new consent required

- The right to withdraw consent

(data must be deleted if data subject no longer wants its data to be processed)

Big Data & Data Protection - issues

Principle of data minimisation vs. collecting as much data as possible

- Finding a correlation or pattern does not retrospectively justify obtaining the data in the first place!

Anonymisation?

- Absolute anonymisation is likely impossible -> focus on mitigating risks of re-identification
- Pseudonymisation = security measure

Health data

Health data is special category of data - processing prohibited UNLESS

***Explicit* consent** (likely to be sole legal ground in the future)

OR

Medical treatment exemption:

Processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, **and** those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

Scope of ‘health data’?

European Court of Justice in Case C-101/01 (*Lindqvist*):

‘In the light of the purpose of the directive, the expression “data concerning health” used in Article 8(1) thereof must be given a wide interpretation so as to include information concerning all aspects, both physical and mental, of the health of an individual.’

Letter of WP29 of 5 February 2015 on data collected by mHealth apps. Health data includes:

- Medical data: ‘data about the physical or mental health status of a data subject (…) generated in a professional, medical context
- Health related data used in an administrative context (information to public entities)
- Data about the purchase of medical products and services provided that the health status can be determined

Future scope of ‘health data’

The scope will be wider as it will include any information about ‘disease risk’.

WP29: ‘disease risk’ refers to

- Data concerning the potential future health status
- Data, which may not necessarily be health data, with the purpose of identifying disease risks (medical research, using big data)

Whether the device or software is a medical device or not is not relevant for the qualification ‘health data’!

- Combination of data aimed to infer health status or health risk?

-> health data

- Conclusion about person’s health status or health risk?
  Conclusion = health data

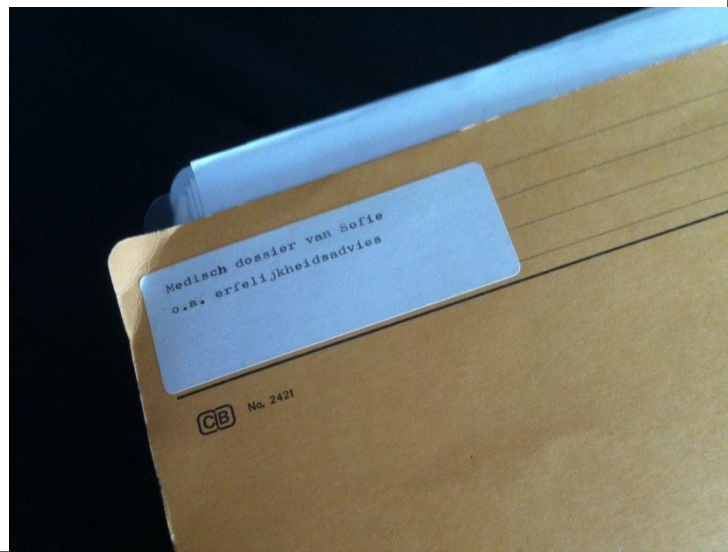
Retention of health data

Retention of personal data: no longer than strictly necessary

Netherlands: 15 years under the Medical Treatment Agreements Act ('WGBO')
(Article 7:446 – 7:468 Dutch Civil Code)

The healthcare professional has to keep a file regarding the treatment of a patient. Retention period of this file is 15 years.

Consent to medical treatment ≠ consent to processing data!!



Security

Data controllers and processors should implement appropriate technical & organizational measures to protect data from loss or any form of unlawful processing.

No specific security measures are mentioned, however security measures should take into account:

- Nature of the data to be protected
- State of the art
- Aim to prevent unnecessary collection and further processing of personal data
- Overriding principle: Plan-Do-Check-Act
- Social engineering?

https://www.youtube.com/watch?v=ecZL4Q2EVuY

The Guardian 30 december 2014

Hacker fakes German minister's fingerprints using photos of her hands

Jan Krissler used high resolution photos, including one from a government press office, to successfully recreate the fingerprints of Germany's defence minister

The hacker used commercial Photograph: A. T. Willett / Alamy/Alamy

Data breaches?
Latest developments NL

Legislative proposal amending the Data Protection Act and Telecommunications Act by incorporating a notification obligation for data controllers in case of data breaches.

The Data Protection Authority can impose administrative fines up to EUR 810.000 in case of violation of the notification obligation.

Notification obligation applies if:

- Security breach
- Entity in public or private sector (companies, governmental organizations)
- The infringement leads to a significant risk of adverse impact on the protection of personal data processed by the organization (theft, loss or abuse of personal data).

Status: adopted by the House of Representatives, currently pending approval of the Senate.

Dutch DPA & security of health data

Conclusion in Annual report 2013 of the Dutch Data Protection Authority:

‘Security of health data not up to standards’

1. DPA Report related to Okki-app in September 2014

Lessons learned from this report?

- In any case, use SSL for transmitting data over the internet.
- In case of an app that is designed to be used by children under 16 years of age, consent for the processing of personal data has to be obtained from the parents (legal representative).

Dutch DPA & security of health data

2. Report related to network security & protection of health data in a hospital published in November 2014

Lessons learned from this report?

- Ensure an overview of all the software and when the software is end of life.
- Timely updates of the software and replacement of end of life software that is no longer supported by the supplier.
- If replacement of end of life software is not possible, take additional measures such as separating the network, disconnecting from the network or implement strict access control to reduce security risks.
- Use proactive monitoring of the network to detect abnormal behavior of users and systems.
- Perform periodic penetration tests to detect vulnerabilities in systems and equipment and take measures to remedy the vulnerabilities.
- Check the terms and conditions of software developers and suppliers on updates and security.

Data transfer outside EU & security

- Surveillance practices (PRISM)

Safe harbor for transfer to US?
Safe Harbor Certification merely means that the transfer of personal data to the US is allowed in principle because it demonstrates the adequacy of the US as jurisdiction

- Recent Facebook case invalidates Safe Harbor transfer mechanism

- Alternatives:

    - Data transfer agreement based on European Commission's standard contractual clauses
    - Binding corporate rules blessed by a DPA

Data transfer outside EU & security

Safe Harbor Ruling Continues To Ripple Through Business Community

Daily Dashboard | Europe Data Protection Digest | Oct 8, 2015

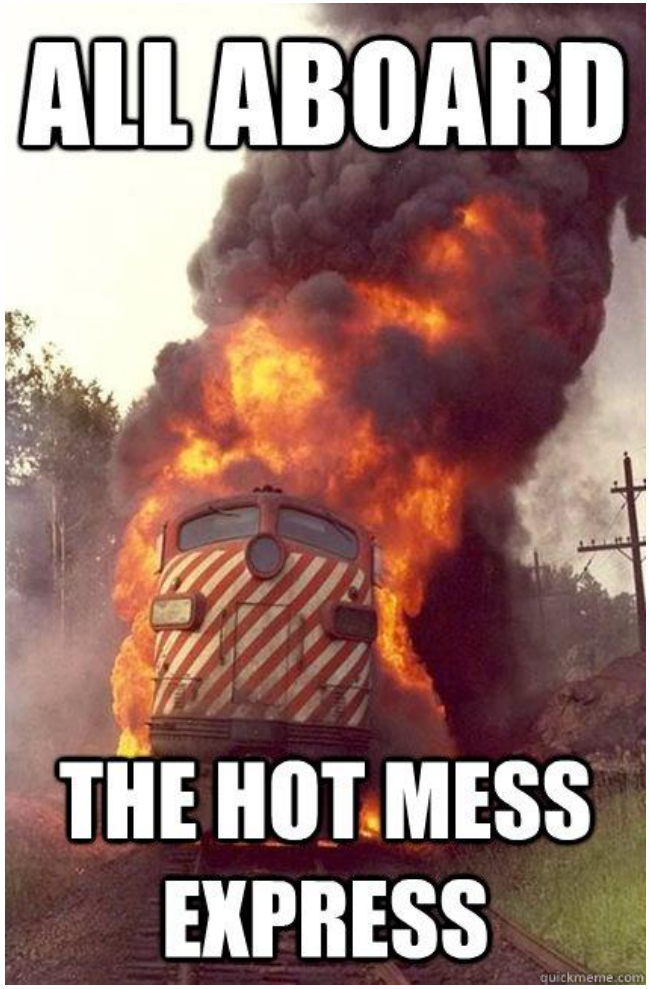
There's no shortage of media coverage of this week's invalidation of Safe Harbor by the European Court of Justice (ECJ). Though many large companies appear to be prepared for other workarounds, small- and medium-sized companies, including marketers and healthcare companies, are feeling the pressure and confusion stemming from the end of this major data transfer agreement. According to *International Business Times*, the decision could spur the U.S. Congress to update its privacy laws. Center for Digital Democracy's Jeffrey Chester said, "There's a conflict here that can't be satisfied until the United States passes a privacy law that includes fair information practices and creates clear rules on digital privacy." A post on *Lawfare* contends that surveillance reform is needed for a revived Safe Harbor. The ECJ decision also further highlights the complexity and importance of the pending Department of Justice case against Microsoft, according to *Bloomberg Business*.

Safe Harbor Fallout: Commission, Council Debate Parliament; German DPA Takes Next Step

Sam Pfeifle

The Privacy Advisor | Oct 14, 2015

General Data Protection Regulation



The current EU system is:

- Fragmented
- Outdated
- Unclear

Proposal for a new framework:
The General Data Protection Regulation.

- Regulation: direct effect in member states (no national legislation)

In force? 2016?

GDPR

- Informed consent and burden of proof it was obtained
- Privacy by design – software & devices have to be designed and built as to enable GDPR and data subject's rights by default
- High fines (up to 5% annual WW turnover)
- Privacy officers mandatory for large companies
- Privacy impact assessment mandatory for each act of processing

Extraterritorial jurisdiction:

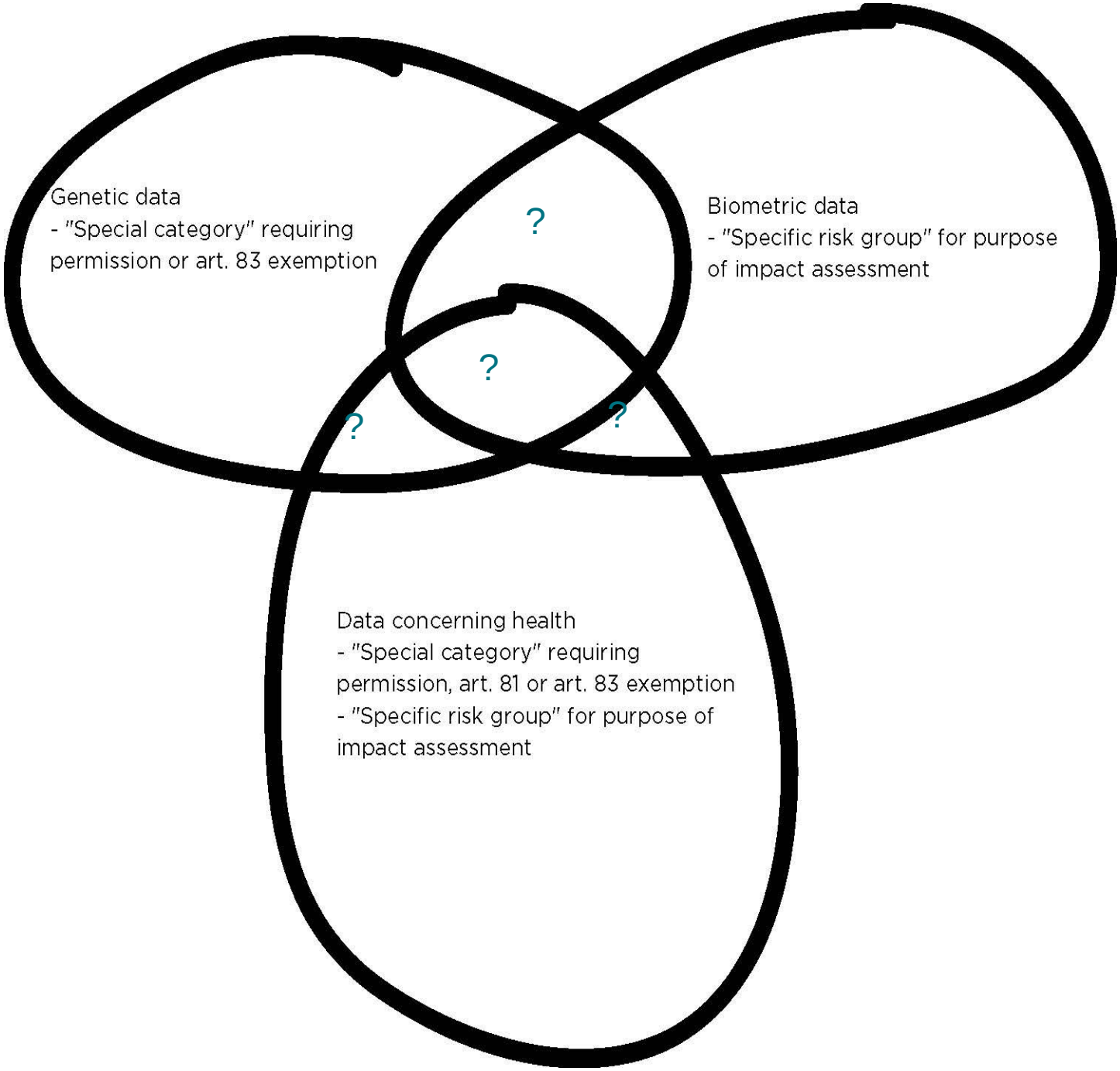
- Data controller or processor established in the EU, whether the processing takes place in the Union or not
- Data controller or processor not established in the EU, if processing is related to:
    - Offering goods or services to data subjects in the Union
    - Monitoring of data subjects in the Union

GDPR – important definitions

- Article 4 (10) 'genetic data'
  "all data, of whatever type, concerning the characteristics of an individual which are inherited or acquired during early prenatal development"

- Article 4 (12) 'data concerning health'
  "any information which relates to the physical or mental health of an individual, or to the provision of health services to the individual"

Clarification is needed around 'genetic data' and 'data concerning health' to ensure that these definitions are only intended to apply to personal data that falls within these categories, rather than all related data.


Genetic data
- "Special category" requiring permission or art. 83 exemption
Biometric data
- "Specific risk group" for purpose of impact assessment
Data concerning health
- "Special category" requiring permission, art. 81 or art. 83 exemption
- "Specific risk group" for purpose of impact assessment
?
?
?
?

GDPR – processing of personal data

Processing of genetic data or data concerning health (article 9)

- only with consent; OR
- processing of data concerning health is necessary for health purposes and subject to conditions and safeguards (Article 81); OR
- processing is necessary for historical, statistical or scientific research purposes subject to conditions and safeguards (Article 83)
- controller has burden of proving that the data subject has given the consent to the processing operation
- consent is not a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller (likely: HCP / patient relation)

GDPR – right to erasure

- The right to withdraw consent and right to erasure (Article 17 GDPR)

Difficult to implement if data is stored in archived backups

- Real risk that statistical analyses will be “depowered” as a result of such changes as result of exercise of rights (particularly in the case of orphan diseases or conditions with difficult inclusion and exclusion criteria, such as paediatratic), thereby calling into question existing registrations (let alone future developments).
- Council general approach addresses this up to a point, but not in relation to commercial big data applications in health

GDPR – when?

Albrecht on GDPR: Very Possibly Done by End of Year

Daily Dashboard | Oct 13, 2015

In a meeting of the European Parliament's Civil Liberties Committee (LIBE), Vice Chairman Jan Philipp Albrecht, Green MEP and rapporteur to the General Data Protection Regulation (GDPR), provided a report on the trilogue negotiations around the GDPR. Chapter five is done, he said, and chapters two, three and four are largely complete. "My impression is that we managed to get agreement on, I would estimate, 70 to 80 percent of the text," he said, adding issues like consent conditions, data minimization definitions and the duties for controllers and processors have yet to be finalized. Albrecht said it's "realistically possible" negotiations will conclude before end of year, Sam Pfeifle reports for *The Privacy Advisor*.

Full Story

GDPR: threatening healthcare

THE PARLIAMENT
POLITICS, POLICY AND PEOPLE MAGAZINE

ENHANCING GOVERNANCE THROUGH INTERNAL AUDIT

Home | Content | Policy | Magazines | PM+ | Thought Leader | Events | Stakeholder Reports | Press Releases | Editorial

PM+: One-time consent on data protection rules a 'necessity' for European health research

Written by **John Crown** on 13 March 2015 in **Opinion Plus**

The risk of potentially damaging consequences to Europe's health research if EU policymakers don't get Europe's data protection rules right is clear, argues John Crown.

THE PARLIAMENT
POLITICS, POLICY AND PEOPLE MAGAZINE

Published on *The Parliament Magazine* (https://www.theparliamentmagazine.eu)

Home > PM+: EU data rules threatening health research

PM+: EU data rules threatening health research

Written by Paolo G. Casali on 23 September 2014 in Opinion Plus
Opinion Plus

'Balance' needed on patient consent, argues Paolo Casali.

CPME

hope
European Hospital and Healthcare Federation

FEAM

COCIR

efpia

GSMA

Continua
HEALTH ALLIANCE

Healthcare Coalition on Data Protection

Amendments to the Commission's proposal for a General Data Protection Regulation

THANKS FOR YOUR ATTENTION

Erik Vollebregt
Axon Lawyers
Piet Heinkade 183
1019 HC Amsterdam
T +31 88 650 6500
F +31 88 650 6555
M +31 6 47 180 683
E erik.vollebregt@axonlawyers.com
@meddevlegal
B http://medicaldeviceslegal.com

READ MY BLOG:
http://medicaldeviceslegal.com

AXON
science based lawyers

www.axonlawyers.com