Universitat Autònoma de Barcelona

PRIVACY AND DATA PROTECTION IN THE EU

19 SEPTEMBER 2019

Dr Cristina Blasi Casagran
Autonomous University of Barcelona

SUMMARY

PRIVACY V DATA PROTECTION

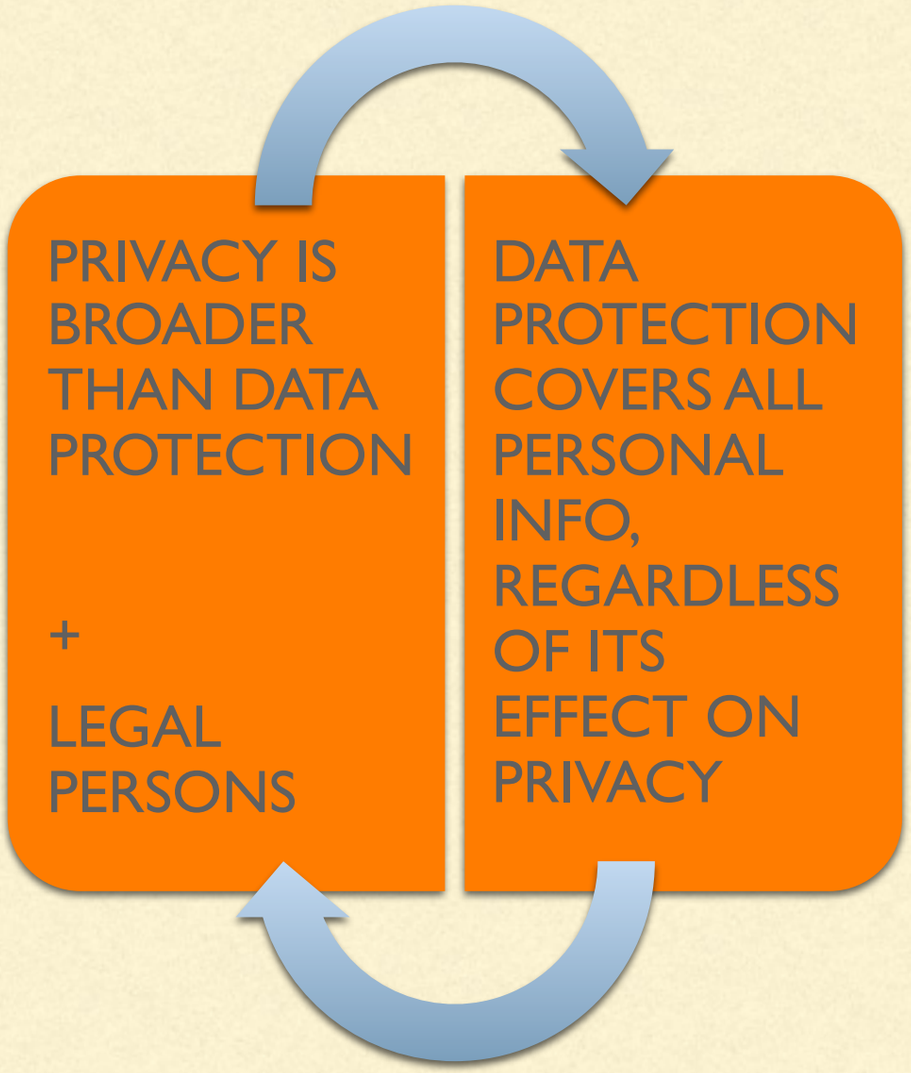
Privacy

Data Protection

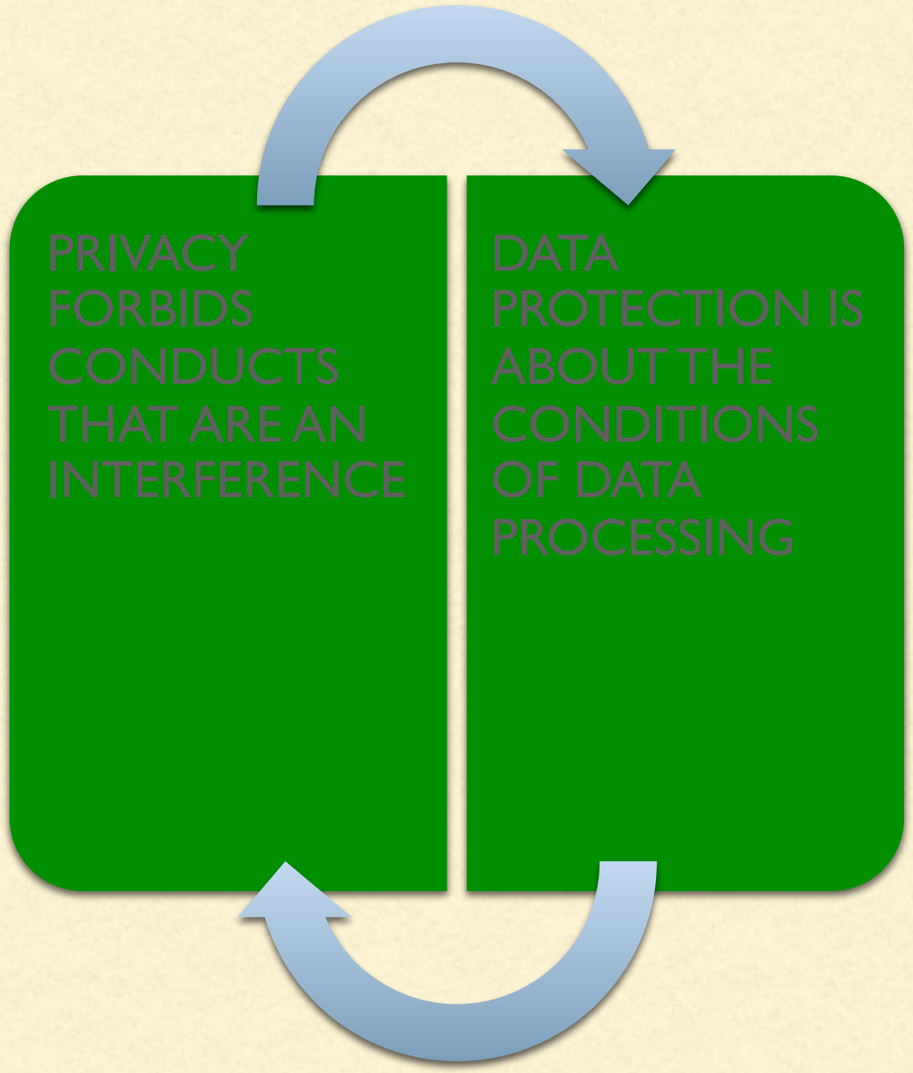
IDENTIFIED OR IDENTIFIABLE NATURAL PERSON

DIFFERENCES PRIVACY – DATA PROTECTION

SCOPE

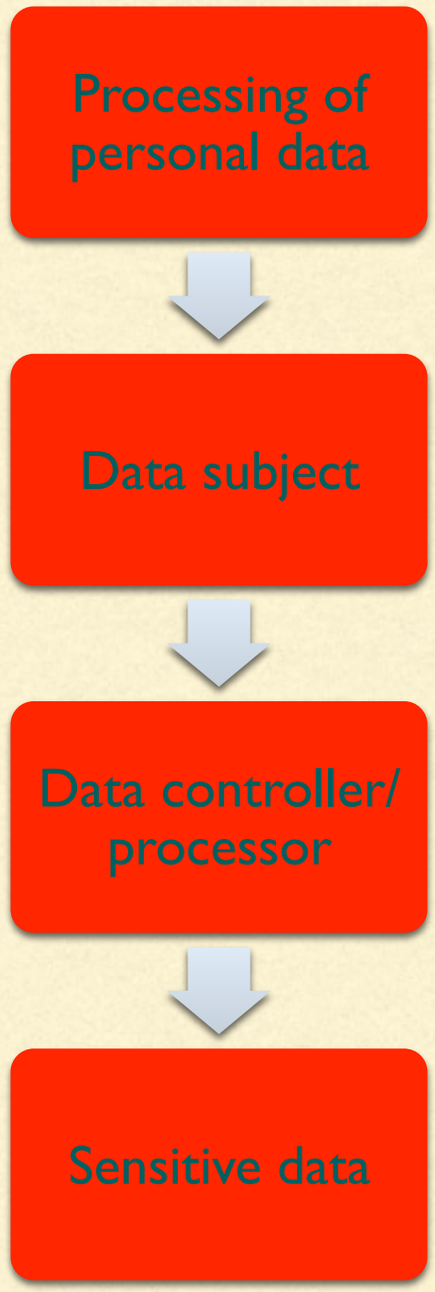


LIMITATIONS



BREYER CASE

OTHER KEY CONCEPTS:



EXAMPLE

SENSITIVE DATA

CoE Convention 108

Race or ethnic origin

Political opinions, religious or other beliefs

Health or sexual life

Criminal convictions

GDPR

Trade union membership

Genetic and biometric data

Sexual orientation data

ORIGINS OF EU DATA PROTECTION LAWS

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

EUROPEAN UNION

COUNCIL OF EUROPE

108 Convention (1981)

ECHR (1953)

ECHR

- Article 8 – Right to respect for private and family life

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

- 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection

108 COE COVENTION

- Object and scope: “automatic processing of personal data”
- Exceptions
- **Principles**: Lawful data collection,legitimate purposes, adequacy, accuracy, data retention limitations.

TREATY OF LISBON

Art. 16 TFUE

Art. 39 TUE

Art. 7 and 8 Charter of Fundamental Rights

Art. 8 ECHR

Declaration 21 Treaty of Lisbon

CHARTER OF FUNDAMENTAL RIGHTS

- Art 7. Respect for private and family life

- Everyone has the right to respect for his or her private and family life, home and communications.

- Art 8. Protection of personal data

- Everyone has the right to the protection of personal data concerning him or her.

- Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which ahs been collected concerning him or her, and the right to have it rectified.

- Compliance with these rules shall be subject to control by an independent authority.

Data protection and privacy TODAY

Directive 95/46/EC → GDPR (2016)

European data protection regulation

- Applies to companies wherever they are based
- Gives citizens control over personal data
- Simplifies the regulatory environment for business

#EUJustice

DIRECTIVE 95/46/EC

Territorial scope

DATA CONTROLLER ESTABLISHED IN ONE OR MORE MEMBER STATES

Core values

- i) the collection limitation principle
- ii) the data quality principle
- iii) the purpose specification principle
- iv) the use limitation principle
- v) the security safeguards principle
- vi) the openness principle
- vii) the individual participation principle
- viii) the accountability principle.

NEW LEGISLATION

- “Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)”

- “Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (Police and Criminal Justice Data Protection Directive).”

WHY A REFORM?

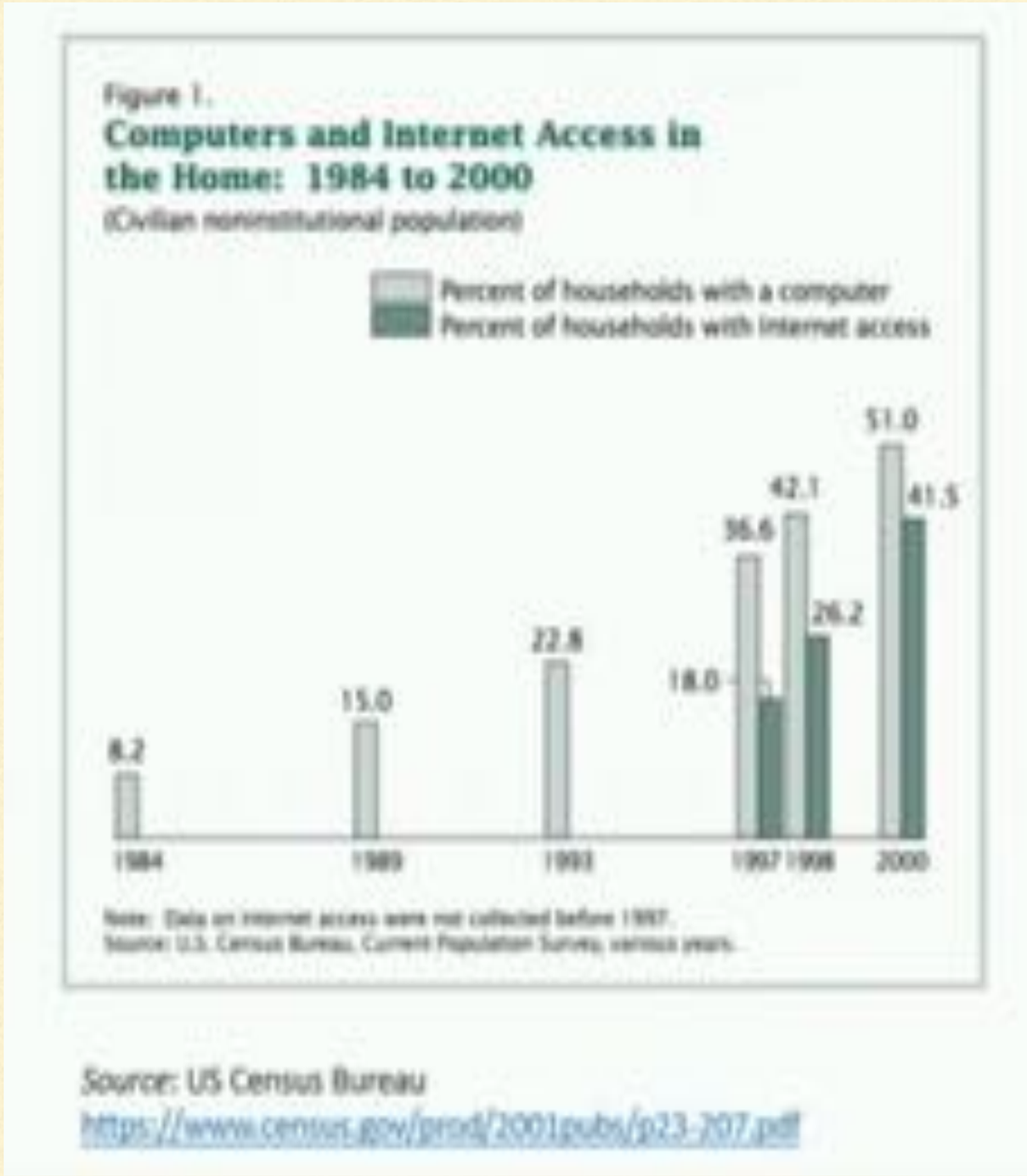


Figure 1.
Computers and Internet Access in the Home: 1984 to 2000
(Civilian noninstitutional population)

Percent of households with a computer
Percent of households with internet access

8.2
15.0
22.8
18.0
35.6
42.1
26.2
51.0
41.5
1984
1989
1993
1997
1998
2000

Note: Data on internet access were not collected before 1997.
Source: U.S. Census Bureau, Current Population Survey, various years.

Source: US Census Bureau
https://www.census.gov/prod/2001pubs/p23-207.pdf

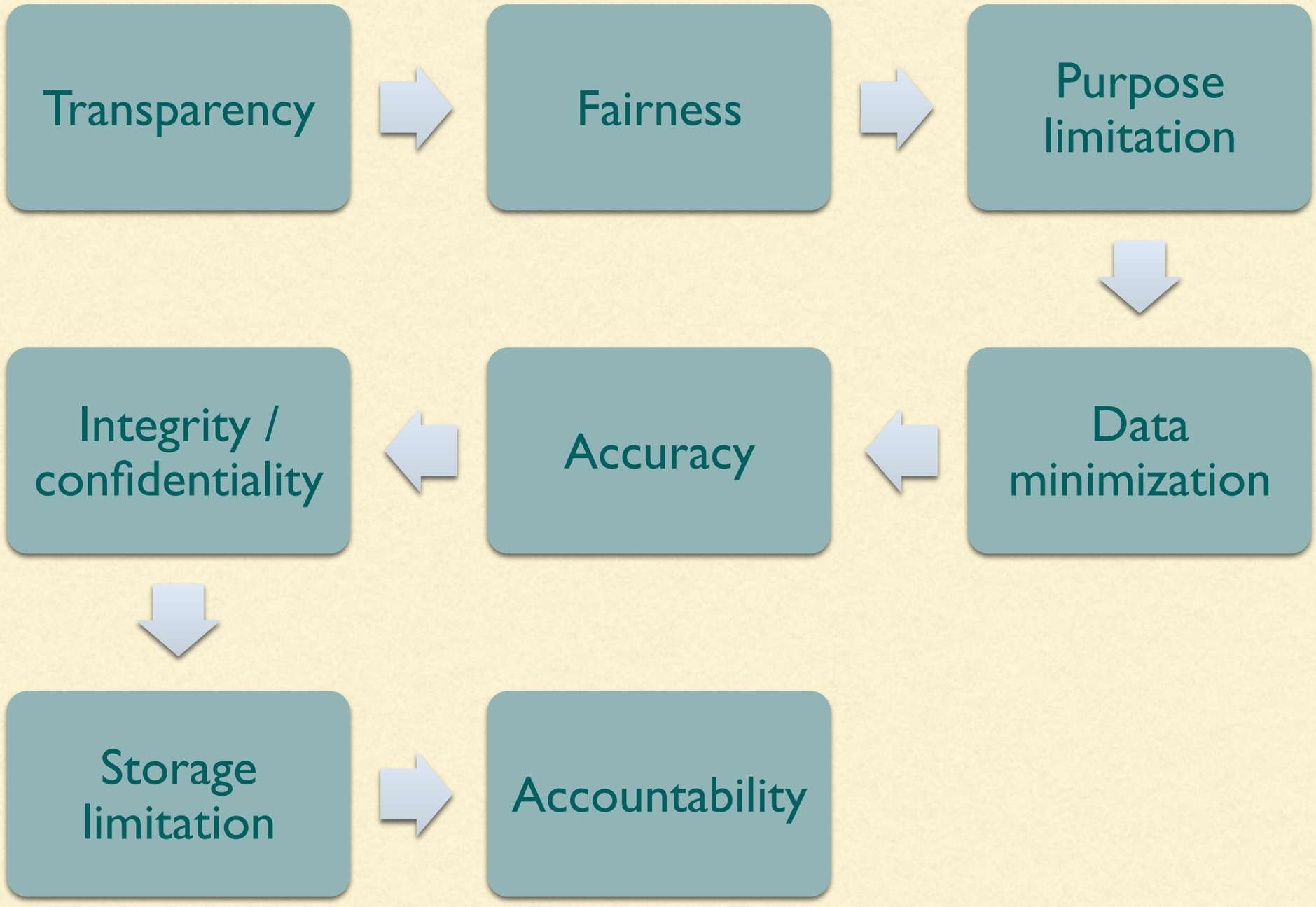
NEW LAW:

- https://www.youtube.com/watch?v=UdWkFloDbAs

NATURE


#1 – It's a Regulation!
VS.
Directive
Instrument passed at EU level
National implementation ("cloning")
Local variations ("genetic variances")
Regulation
Instrument passed at EU level
No need for national implementation
"One ring to rule them all"

PRINCIPLES


Transparency
Fairness
Purpose limitation
Data minimization
Accuracy
Integrity / confidentiality
Storage limitation
Accountability

CONVENTION 108+ (NEW PROTOCOL, MAY 2018)

Signed by Austria, Belgium, Bulgaria, Czech Republic, Estonia, Finland, France, Germany, Ireland, Latvia, Lithuania, Luxembourg, Monaco, Netherlands, Norway, Portugal, Spain, Sweden, the U.K., and by Uruguay.

Same **principles** as those enshrined in the new EU data protection rules

- **Recital 105** of the GDPR states:

- "The Commission should take account of obligations arising from the third country's participation in multilateral or regional systems in particular in relation to the protection of personal data, as well as the implementation of such obligations. In particular, the third country's accession to the Council of Europe Convention 108 and its Additional Protocol should be taken into account."

EXTRA-TERRITORIALITY

#3 – It has extra-territoriality!

- Current law applies if establishment or equipment in the EU.
- New law applies if:
  (a) establishment in the EU
  (b) offer goods and services to EU residents
  (c) monitor behaviour of EU residents

- Companies w/o presence in EU will need to comply!

DATA PROCESSORS

#4 – It applies to processors!

Current law = no obligations on processors (i.e. service providers)

New law = direct accountability obligations on processors

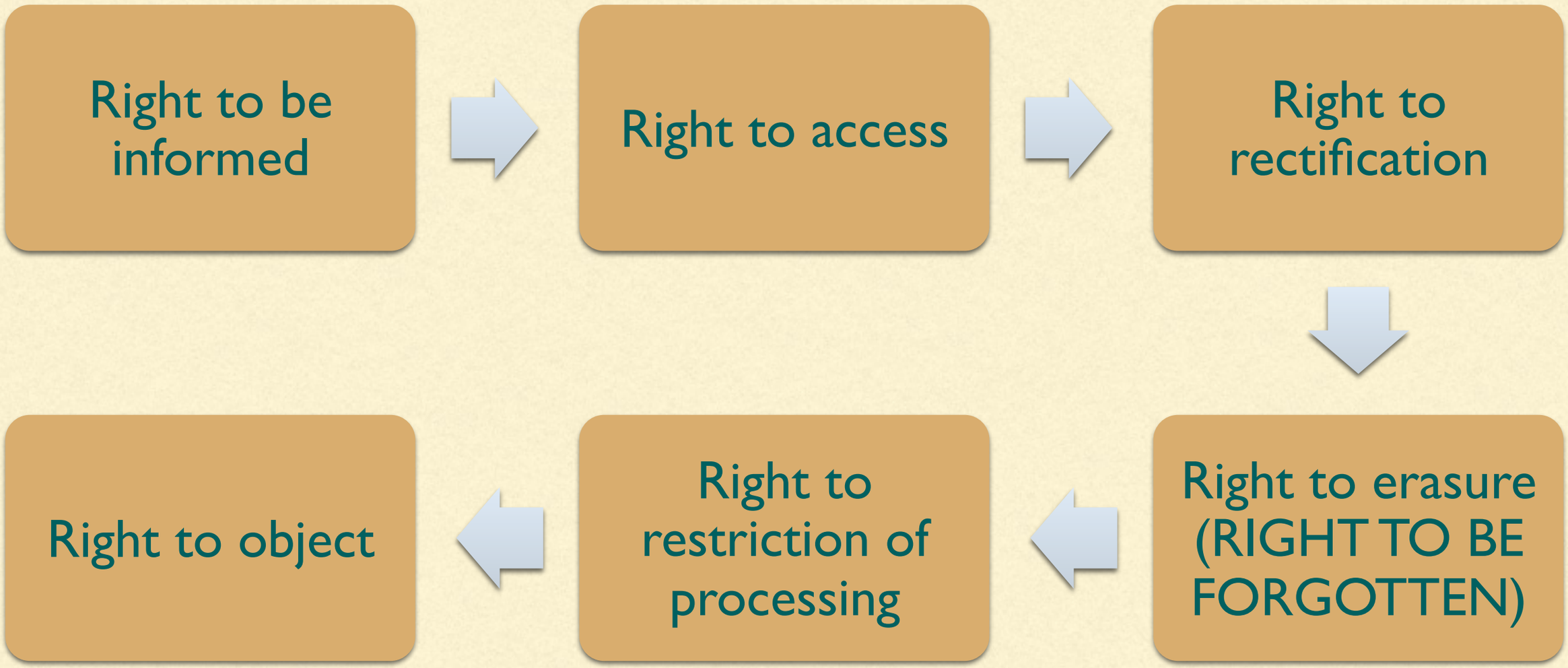
Plus mandatory terms for all controller / processors / subprocessors?!!

Major impact on cloud industry?

CONSENT

- Free
- Informed
- Specific
- Unambiguous
- (Explicit)

DATA SUBJECT RIGHTS



GOOGLE SPAIN CASE

DATA BREACHES

#7 – Data breaches must be notified!

No pan-EU data breach reporting rules currently
(unless ISP/telco)

New law introduces breach reporting requirements to:

(a) data controllers (if you're a data processor)

(b) regulators

(c) affected data subjects (unless low risk of harm)

Generally expected to report within 72 hours?

DATA BREACH NOTIFICATION

Article 33

Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

FURTHER NOVELTIES

OTHER RIGHTS

DATA PORTABILITY

OTHER NEW CONCEPTS

PROFILING

DATA PROTECTION BY DESIGN AND BY DEFAULT

EXAMPLE PRIVACY BY DEFAULT / DESIGN

- **VIDEO:**

Nepcom

- https://www.youtube.com/watch?v=BRs1xpMi1mg

EXAMPLE PROFILING

Huge new screen in London's Picadilly Circus will display ads based on nearby cars and people

Smile, the brands are watching

Landsec says hidden cameras will analyze the make, model, and color of cars that drive by as well as the age, gender, and even the feelings of nearby pedestrians in order to customize ads for the local audience. The technology can be used to program certain ads to play when specific cars drives past, for example, or in response to weather changes, or news and sport reports. The new screen will also provide complimentary Wi-Fi for people in the surrounding area.

DPO

#8 – You'll need a Data Protection Officer!

- No requirement to appoint a DPO under the current law
- New law = requirement for controllers and processors
- Threshold for appointment:
  (a) Mandatory for public authorities
  (b) 'large scale' systematic monitoring of individuals
  (c) 'large scale' processing of sensitive data
- Can be employee or outsourced DPO

FINES /DPAS

Fines up to 10.000.000 euros or up to 2% of the total worldwide annual turnover of the preceding financial year.

- Obligations controller / processor
- Obligations of certification body
- Obligations of monitoring body

Fines up to 20.000.000 euros or up to 4% of the total worldwide annual turnover of the preceding financial year

- Data processing principles
- Consent
- Data subject's rights
- International data transfers

EXAMPLE

- Early 2018: The Portuguese Supervisory Authority fined an unnamed hospital **400,000 euros** for violations of the EU General Data Protection Regulation. The CNPD found in its investigation hospital staff members illicitly accessed patient data through false profiles. The hospital only had 296 registered doctors; however, the organization's profile management system listed 985 accounts. Even though Portugal has not officially implemented the GDPR, the CNPD still used the rules to determine the fine against the hospital.

ONE-STOP SHOP MECHANISM

Local DPA (Concerned DPA)

Lead DPA

EDPB

Pre-conditions

Data subject need to be established within the EU

Processing of data has been carried out by a private company (no public entities)

- Thanks for your attention