



# The GDPR & Personal Information Management Systems

1. What is data protection law
2. Before the GDPR: the Data Protection Directive
3. The GDPR: most important changes
4. Personal Information Management Systems

# What is data protection law

= law designated to protect our personal information

Gained momentum when **OECD** developed privacy guidelines

- Before: several national legislations contained some data protection principles
- Guidelines contain privacy principles:
  - Collection limitation principle
  - Data quality principle
  - Purpose specification principle
  - Use limitation principle
  - Security safeguards principle
  - Openness principle
  - Individual participation principle

# Before the GDPR: Data Protection Directive 95/46/EC

Enacted in 1995

First attempt to harmonize European data protection law

Introduces new concepts like data controller & data processor

- **Data 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
- **Data processor:** natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller

Introduces the data protection principles

- Fair and lawful processing
- Purpose specification
- Data minimization
- Data quality
- Individual participation

Revision was called for in 2011

# The GDPR: most important changes

Extended territorial scope

New definitions (extra)

New basic principles

consent by children

New obligations for controllers

New rights for data subjects

Fines

Added clarifications

# Extended territorial scope

Art 3.1 & 3.2. GDPR: “This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

the monitoring of their behaviour as far as their behaviour takes place within the Union.”

- In line with **Google Spain, Weltimmo** (extra)
- Data protection law applicable no matter where processing takes place
- Solves the issue of lack of jurisdiction over third country controllers processing European data

# Google Spain

Facts: Mr. Costeja González wanted information about his bankruptcy removed from the results list generated by Google. Google claimed it was not within the ambit of the DPD, there was no personal data involved, that it wasn't a data controller and that a right to erasure did not exist.

- CJEU: Google IS within the scope of the DPD
  - Google Spain is an establishment of Google Inc.
- CJEU: there IS a right to erasure if the processing of data is inadequate, irrelevant or excessive.
  - ➔ Right can now be found in the GDPR.

## New definitions – art 4 GDPR (1)

**Biometric data:** “personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data”

**Genetic data:** “personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained”

**Health data:** “personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status”



## New definitions – art 2 GDPR (2)

**Pseudonymisation:** “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”

**Binding corporate rules:** “personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity”

**Personal data breach:** “breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed”

# New basic principles

**Transparency:** additional compliance obligation

**Accountability:** the controller must keep records himself vs. previous prior notification obligations in DPD

- Art 5, 24 & 30 GDPR
- Less red tape for companies

**Data protection by design & default:** new technical measures to ensure GDPR compliance are required

- Privacy and data protection should be key consideration from the start of any project

# Consent by children

art 8 GDPR

Consent by children under 16 must be given by parent.

BUT Member States may lower the age to 13.

- So far, the UK & Ireland: 13, Spain: 14
- Other MS with plans to change age: Sweden & Poland



# New obligations for controllers (1)

## Format requirements for **communication** with data subjects

- Clear and plain language + understandable format

## New **information** requirements

- the contact details of the controller, the controller's representative (if any) and the DPO; legal basis for the processing; the controller's or a third party's legitimate interests based on which the processing is carried out; information about the source of the personal data (if not collected from the data subject) and whether it originates from publicly accessible sources; and the period during which the personal data will be stored
- obligation to inform the data subject about the latter's rights to: obtain erasure of the personal data, obtain restriction of the processing, object to the processing, have data portability, lodge a complaint with the supervisory authority and withdraw consent to the processing at any time, know about intention to transfer data to a third country or an international organisation

# New obligations for controllers (2)

## New ground for obligations

- Data protection by design and default

## Designation of a data protection officer

- If processing requires regular and systematic monitoring of data subjects OR when special categories of data are processed.
- Tasks are defined in art 37-39 GDPR

## Obligation to maintain records

- Art 30 GDPR
- Maintain records of processing activities

# New obligations for controllers (3)

## Data breach notification

- Stricter data security obligation
- Controllers need to implement appropriate technical and organizational measures (Art 32 GDPR)

## Data protection impact assessment

- In cases of potentially high-risk processing activities
  - Non exhaustive list of activities
- Comes in place of general notification obligation

# New rights for data subjects

Right to erasure: consequence of **Google Spain**

Right to information: expanded considerably. Art 13-14

Right to access: communication in an intelligible form about the processed data + list of information that needs to be given

Right to rectification: of inaccurate or incomplete data.

**→ Contributes to improved control of users over their personal data**

# Fines

2 thresholds:

- Infringement of accountability principle = 10.000.000 EUR 2% of the total worldwide annual turnover
- Infringement of fundamental principles = 20.000.000 EUR or 4% of the total worldwide annual turnover





# Added clarifications (1)

## Position & obligations of processors

- Processing must be governed by contract determining duration, purposes & processed personal data types

## Liability of joint controllers & processors

- Each controller & each processor are held liable for the entire damage caused – art 82 GDPR

## Data minimization principle

- Specified data needs and usage
- Limiting personal data processing to the minimum necessary

# Added clarifications (2)

## Conditions for consent

- given freely and be a specific, informed and explicit indication of his or her wishes
- Controller bears burden of proof

## Criteria for lawful processing

- data subjects' interests or fundamental rights and freedoms are not overridden by the controller's legitimate interests
- Conditions for processing children's personal data



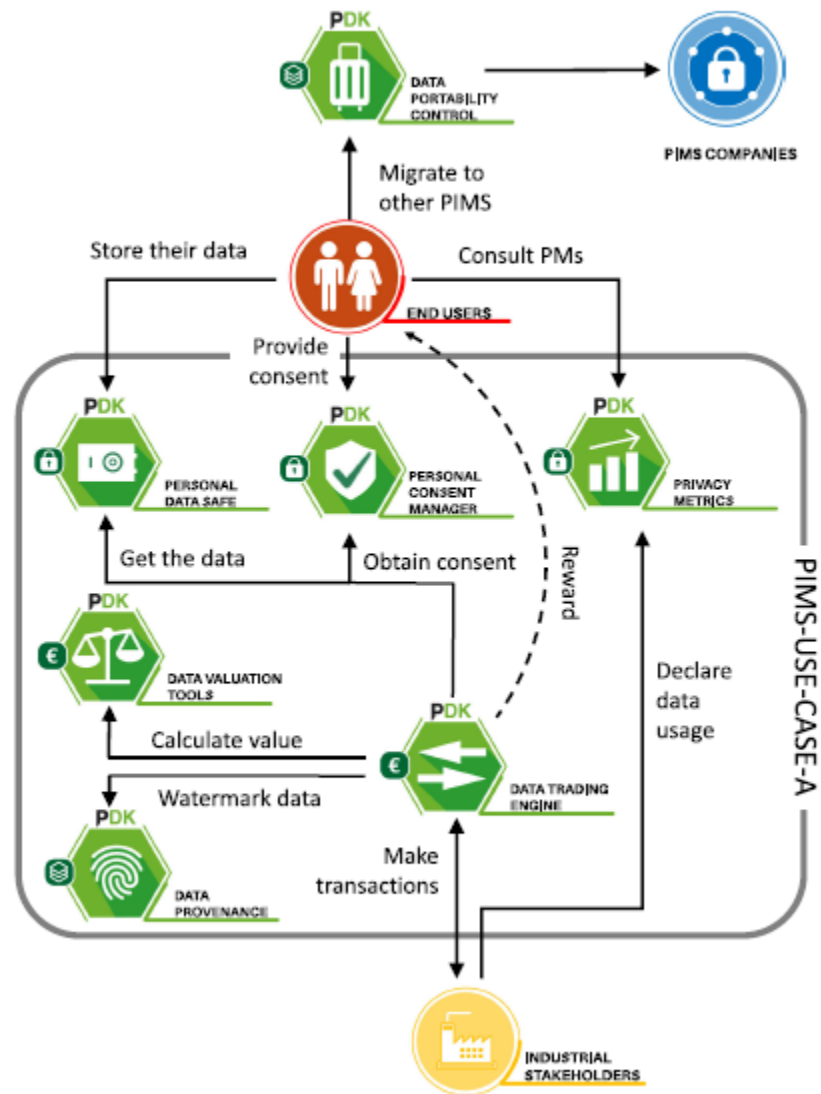
# Personal Information Management Systems

# Content

1. PIMS in general
2. Consent management
3. Data Marketplaces
4. Capacity of parties in a PIMS

# Personal Information Management System (PIMS)

- Provides control for individuals
  - Personal data storage
  - Market place for trading of user data
- Human centric approach to personal information



# Consent Management

- One of 6 legal bases under the GDPR
- Requirements of consent:
  - Freely given (and withdrawn)
  - Specific
  - Informed
  - Unambiguous

Controller must be able to prove this!

Consent must also be given granularly e.g. on specific levels!



## Consent must be given

- Actively (e.g. ticking a box)
- There can be no negative consequences if consent is refused
- No bundling (e.g. together with terms & conditions, which you cannot refuse)
- Must as 'as easy to give as to withdrawn'



# Consent in PIMS

Preferences

		Sociodemographic information	Contact information	Browsing history	Location history	Interests
Commercial purpose		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Research		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

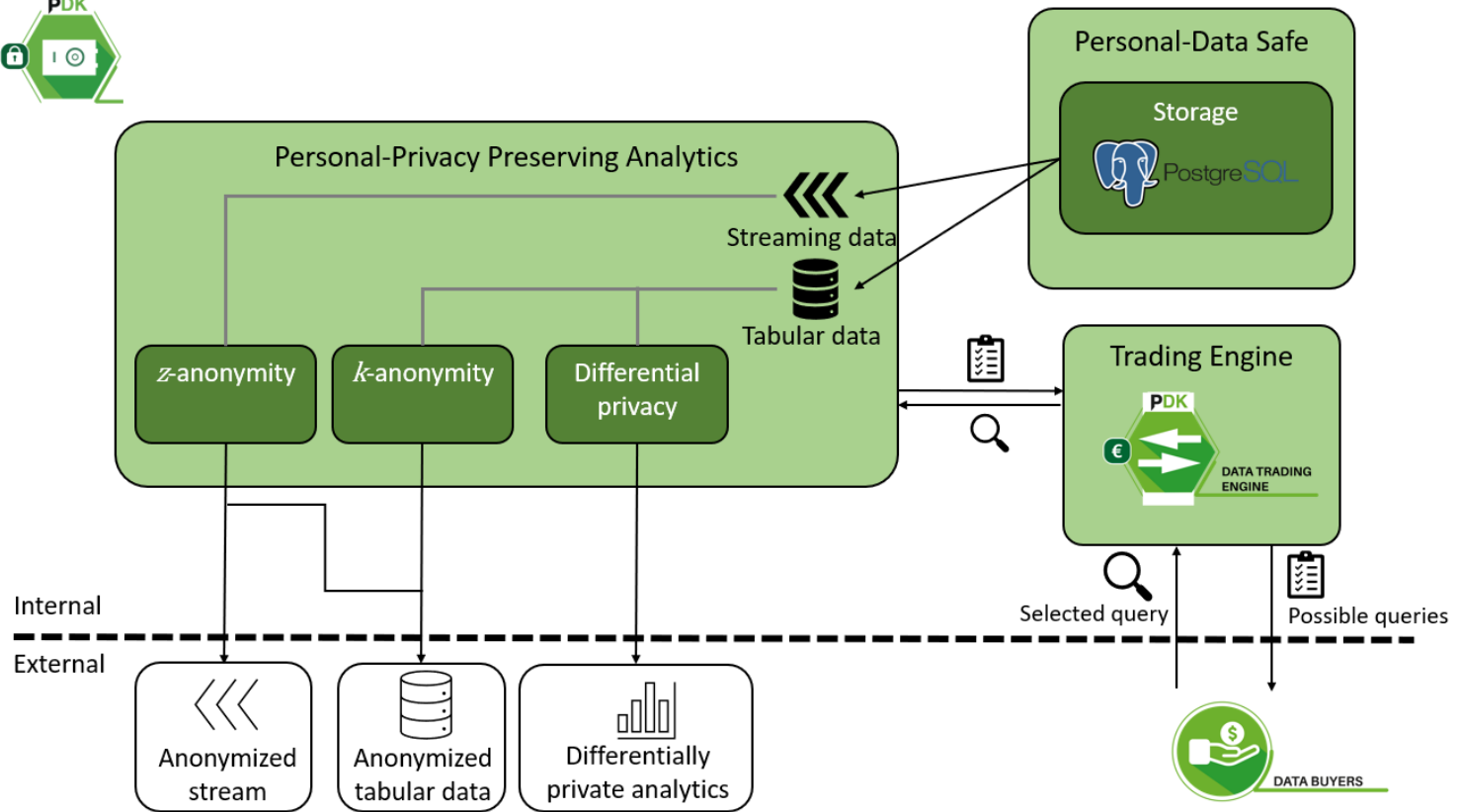
**Interest consents**  
Select interests to share

# Data Marketplaces

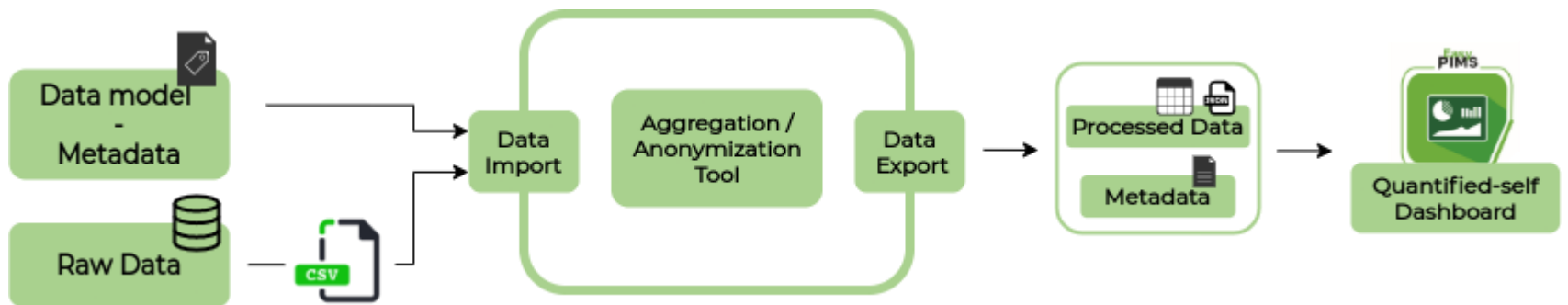
The Data Marketplace brings together user data and data buyers.

Fundamentals:

- Data cannot be shared with the appropriate consent.
- Analytics shown to data buyers *cannot* contain identifying information
- Users must 'trust' the platform if they want to use it



# Anonymity and identity disclosure



How to bring user data to data buyers without revealing identities?

➤ Aggregation of data through anonymity techniques

Information about users get bundled together with lower granularity:

Age 28 – 35 instead of actual age

City level instead of street

Group of interest (e.g. politics) instead of an actual politician

# Does the GDPR apply?

In anonymous data, the GDPR is **not** applicable!

Data is anonymous if it does not relate to an identified or an identifiable natural person.

E.g. a shoesize *on its own*. However, shoesize 49 in a group of 10 people with only one person being very tall constitutes personal data.

Two approaches:

- Relative approach
- Absolute approach

# Relative approach

The relative approach bases itself on:

- Risk of (re)identification
- Type of data (more sensitive, higher risk)
- Means reasonably likely used to reidentify
- Time and resources necessary

➤ Risk based approach towards anonymization

Not often followed by Data Protection Authorities

# Strict approach

If in a dataset:

- links can be established with between individuals/groups (even with another dataset)
- Data can be inferred based on an attribute
- Individuals can be singled out/isolated

Then it is **not** anonymous.

Very strict interpretation. Even if there's a possibility of this happening in the future!



# Impact of aggregation/anonymisation

The more data gets aggregated, the less usable it becomes (trade-off with privacy!). At which point is data not usable anymore?

Even if data is not 'anonymous', it is still an appropriate technical measure to protect personal data.

# Roles of the parties

In a PIMS there are three parties:

- Users (data subjects under GDPR)
- PIMS itself
- Data buyers

The users are not relevant for the next topic.

# Capacities under GDPR

There are three categories a party can fall under

1. Processor
2. Controller
3. Joint-controller

Who is what is depending on who is empowered to determine the purposes and means of the processing of personal data

Controller provides instructions to processor.

Assessment must be done on a case-by-case basis (and trumps contractual clauses)

# Processors

- Receives instructions from controller for their service
- Does not determine the purpose of the processing
- *Can* determine the means (e.g. technical set-up)
- Is **not** allowed to process personal data for their own purpose
  - If they do, they become a controller on their own

Lighter responsibility under the GDPR

# Controllers

- Determines the why and the how of the processing of personal data.
- Gives instructions to controllers
- Carries biggest responsibilities
  - Informing data subjects
  - Due diligence
  - Responsible for technical and organization measures
  - Etc.

# Example

Company X (controller) contracts a cloud service (processor) to host their customer data. The controller X does not decide how the cloud service works, nor how they set-up their technical environment. That is up to the cloud service. It is the controller's duty to perform their due diligence by checking whether the processor complies with the GDPR (among other regulations).

Why the service is a processor:

- It's a separate entity
- Which processes data on the *controller's behalf*

The service receives instructions from company X, which it must follow. Company X decides the purpose (hosting customer data) and decides to outsource this hosting to the service.

# Joint-controller

Joint-controllership arises when two controllers *jointly* decide on the purposes and means of the data processing.

- Converging purposes
- Processing is not possible without both parties
- Parties are inextricably linked

# Case law evolution

- *Wirtschaftsakademie*: creation of a Facebook fan page leads to joint-controllership. Even if not every controller has access to the data or equal responsibility.
- *Jehovah's Witnesses*: Joint-controllership is interpreted broadly: any natural or legal person who, for their own purposes, exerts influence on the processing of personal data. Access to the data is not a relevant detail.
- *Fashion ID*: Implementing a 'like button' plug-in on your website constitutes joint controllership. Regardless of influence on the processing of data.



# IAB Europe vs Belgian DPA

IAB Europe created Transparency & Consent Framework (TCF)

- Consent manager
- Real time bidding protocol

DPA ruled they were controller as they set up a standardized framework data buyers had to comply with in order to use TCF. Without the TCF, data buyers would not be able to reach their goals.

IAB Europe determines the purposes and the means of the processing.

➤ Currently appealed, very impactful on PIMS

# Capacities in PIMS

For a PIMS platform

- PIMS is controller for the data storage
  - Only PIMS determines the purposes and means of processing

For the data buyers

- Data buyer is controller once user has shared their data
- What about the trading engine/data marketplace itself

Unclear!

# Data marketplace

PIMS as a processor of the data buyer

PIMS is (partly) in control, determines the means and purposes of the initial processing.

➤ Processing data for own purposes rules out PIMS being a processor!

# Separate controllers

It could be possible that PIMS and data buyer are controller to controller.

PIMCity is responsible for the set-up and initial processing (data storage). They facilitate the platform.

Data buyer does offers to users, they determine purposes. Users consent to having their data shared. PIMS is not involved as an actor.

Each party is fully in control of their own purposes, no jointly determined purpose. Controller to controller is likely.

Key difference with IAB Europe: they provided an inextricably linked ad ecosystem.

# Joint-controllership

PIMS and data buyer might be joint-controller for the trading of data:

- Jointly determined purpose (the trading)
- Processing is not possible without either of the parties

Open questions

- Is it inextricably linked?
- Does PIMS play a decisive role in the processing (dissemination) of personal data?
- Does a standardised approach and technical protocol which must be adhered to automatically lead to joint-controllership?

Joint-controllership is likely under current case law. Open for debate and not confirmed yet.