PRIPARE

PReparing Industry to Privacy-by-design by supporting its Application in REsearch

Privacy by Design

A technical perspective

Carmela Troncoso

Gradiant

The usual « privacy » scenario

- Protect personal data from third parties

- Data controller is considered **trusted**
  - Data protection to reduce privacy risks
  - But privacy is lost… (Google, Facebook, …)

Privacy by design approach

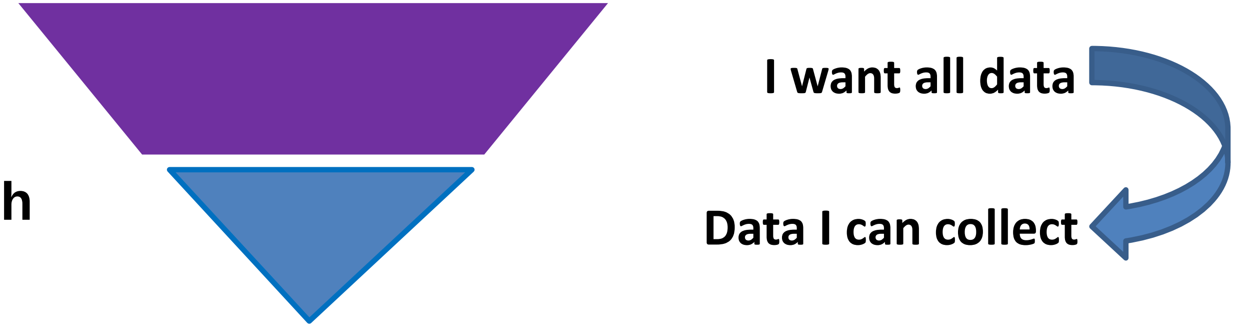
- Protect personal data from **everyone**

- Data controller is considered not **trusted for privacy**
  - Risk reduced by not sharing data
  - No need to trust!

Privacy by design – data minimization

- Collect only necessary data

Usual approach

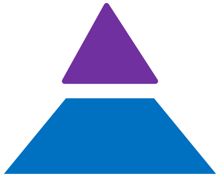


I want all data

Data I can collect

Data protection compliance

PbD approach

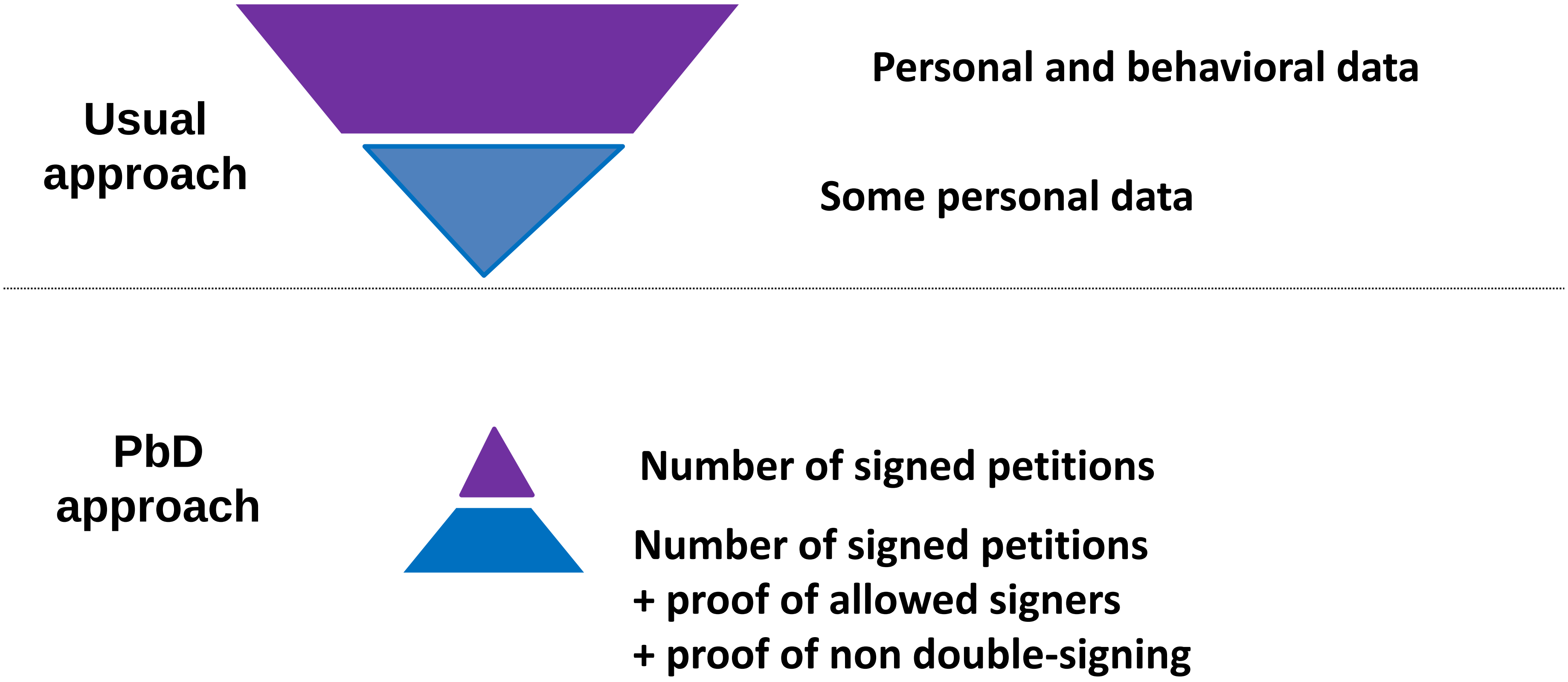


Data that must be output by the system to work

Data I will finally collect (aux data for functionality)

Privacy by design – data minimization

- ePetition example



Usual approach

Personal and behavioral data

Some personal data

PbD approach

Number of signed petitions

Number of signed petitions
+ proof of allowed signers
+ proof of non double-signing

Privacy by design – what data to protect

Usual approach

Personal data/Personally identifiable information (PII):

- Data related to the individual
- Enough attributes to identify an individual (pseudo-identifiers)

PbD approach

+ Privacy-relevant data:

- Enables linkage of actions/attributes (can become pseudo-identifiers)
- Enable discrimination

ENISA report: “Privacy and Data Protection by Design - from policy to engineering” George Danezis, Josep Domingo-Ferrer, Marit Hansen, Jaap-Henk Hoepman, Daniel Le Métayer, Rodica Tirtea, Stefan Schiffner.

Privacy by design – Use of PETs

- Use of PETs to minimize disclosure while enabling functionality

- PbD applications enabled by PETs
  - **Privacy-preserving Pay as you drive/eTolling/smart metering**: local computations and only billing information sent to the server + auxiliary verification information) [cryptographic commitments]
  - **Privacy-preserving ePetition**: eID proving the value of an attribute (person lives in a city) [anonymous credentials]
  - **Privacy-preserving transportation cards**: use transport without being tracked [anonymous eCash]
  - **Privacy preserving statistics**: compute global use statistics without revealing individual consumptions [secure multiparty computation]

Take aways

- Privacy by Design protects privacy from **all** actors in a system

- Data protection alone **is not** privacy by design ☹
  - Should not be an excuse to not apply further protection
  - Consent is not a blanket solution
  - Application purpose must be well defined for proportionality and minimization
  - Anonymization is not trivial...

- But... Privacy by Design still needs data protection
  - Some applications inherently need to collect sensitive data
  - There are also PETs to support data protection (transparency, consent)

PReparing **I**ndustry to **P**rivacy-by-design by supporting its **A**pplication in **RE**search

Thank you for your attention

Questions?

Website: www.pripareproject.eu

Project Co-ordinator	Technical Co-ordinator
Antonio Kung (Trialog)	Christophe Jouvray (Trialog)