DATAIA
10 July 2018

GDP-ERE
GDPR and personal cloud
- from Empowerment to Responsibilities -

Célia Zolynski, Professor UVSQ
Nicolas Anciaux, Inria researcher

Personal data : current trends

From hyper-centralized management of personal data…

Data silos managed by Web majors ➔ security and privacy issues

… to its democratization

Citizen's involvement ➔ empowerment and privacy

1°) Data portability: smart disclosure (US) & GDPR (EU)

Blue Button Download My Data

Green Button Connect My Data

MIDATA

MesINFOS

GDPR, art. 20 & Digital Republic Act (France), art. 48

Freedom to move ➔ Freedom to choose

Personal data : current trends

2°) Emergence of Personal Cloud solutions

cozy.io

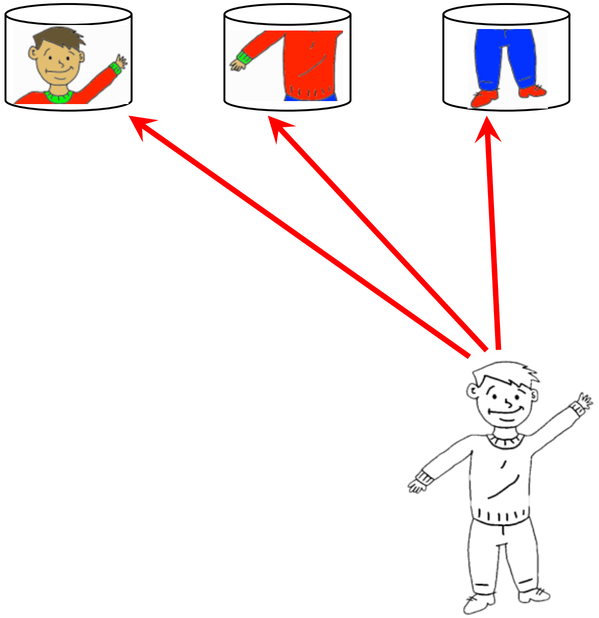
meeco

DATABOX

digi.me

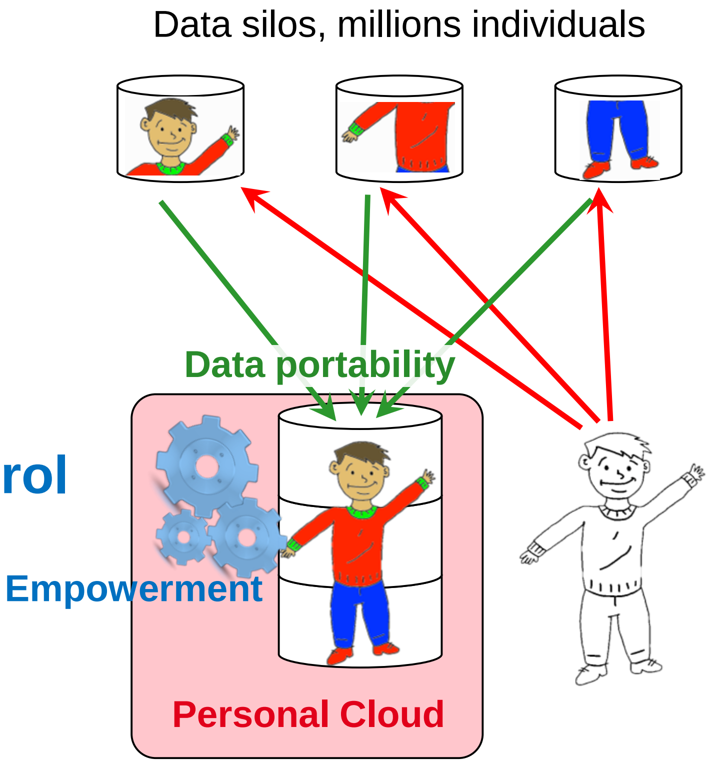
BITSABOUT.ME

Data silos, millions individuals



Personal data : current trends

2°) Emergence of Personal Cloud solutions



Data portability ➔ repatriation of data to users

Empowerment ➔ usage capabilities, under control

Personal data : current trends

2°) Emergence of Personal Cloud solutions

cozy.io

meeco

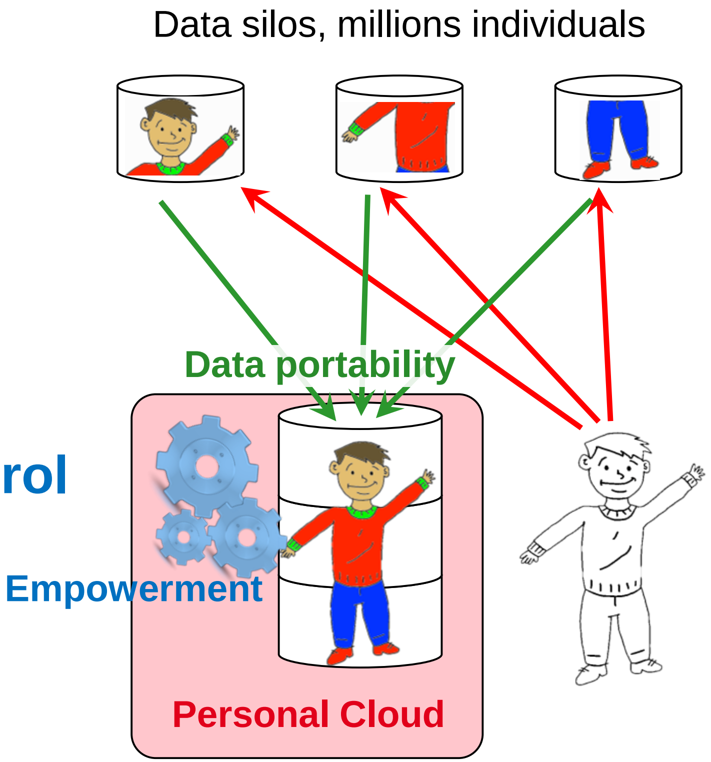
DATABOX

digi.me

BITSABOUT.ME

Data portability ➔ repatriation of data to users

Empowerment ➔ usage capabilities, under control



Holy Grail or Boomerang effects ?

Are empowerment and control guaranteed?

Finally, more or less privacy for the individuals?

GDP-ERE approach

Equation to be verified: Portability x Personal Cloud = Empowerment

Empowerment entails ‘responsibilities’ ➔ Inject it into the equation

1-Problem cases

2-Analisis of State of the Art solutions from the technical & legal angles

3-Solution ingredients studied in the GPD-ERE project

Problem : potential board effects & data leaks

Data storage protection & recovery

- Personal cloud data content is critical
- Bank, health, social, histories… + credentials

Safe data collection (portability)

- Untrusted code (scrapper) manipulate credentials & data
- Connect to a remote site and acts as the user

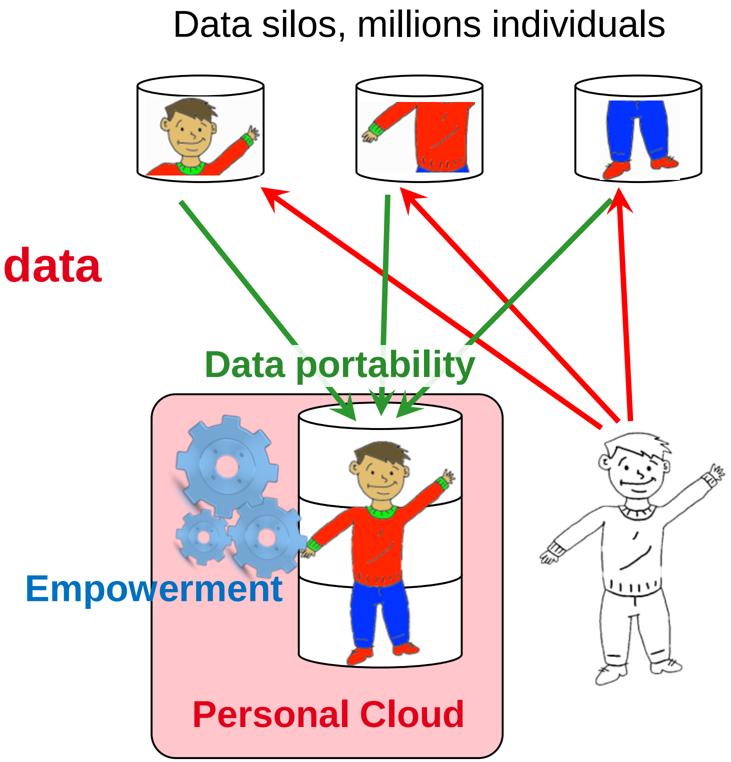
Trusted personal computations

- Trust for third parties: e.g., produce an energy bill
- Trust for the user: access to large sets of raw data

Trusted crowd computations

- Community of patients, energy games, etc.
- Access to the raw data of many participants

A new right ➔ define related responsibilities

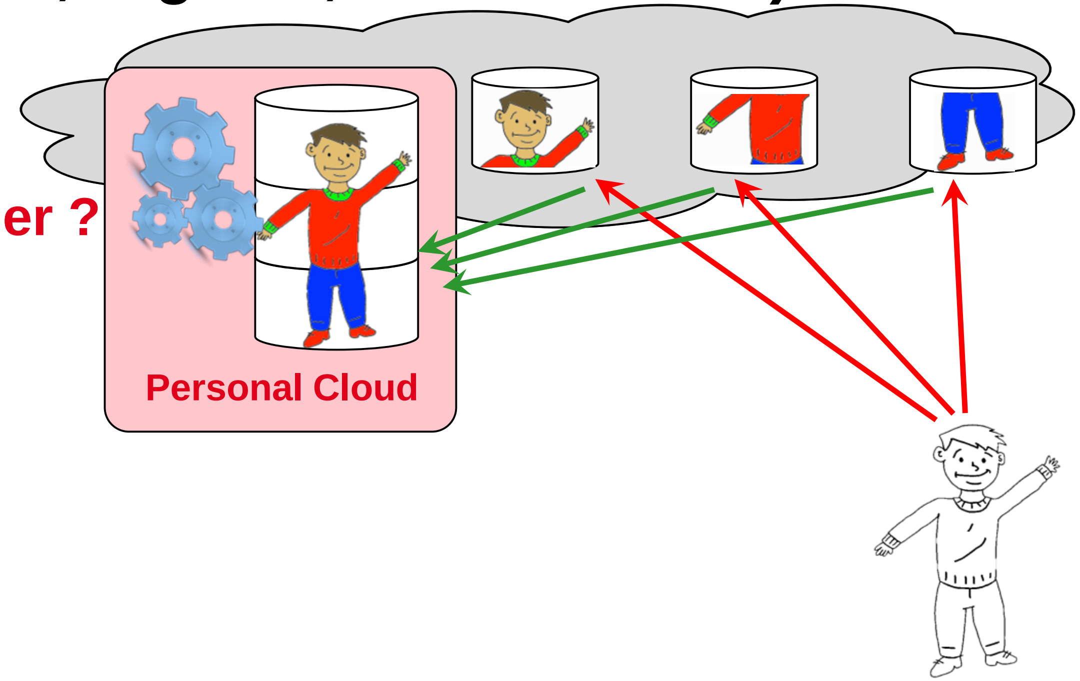


Responsibilities induced by the technical choices ?

Wide variety of architectures, functionality, security

Online solutions (e.g., CozyCloud, Digi.me, BitsAbout.Me)

- The personal cloud provider
- … manages data and applications
- More responsibilities to the provider ?



Responsibilities induced by the technical choices ?

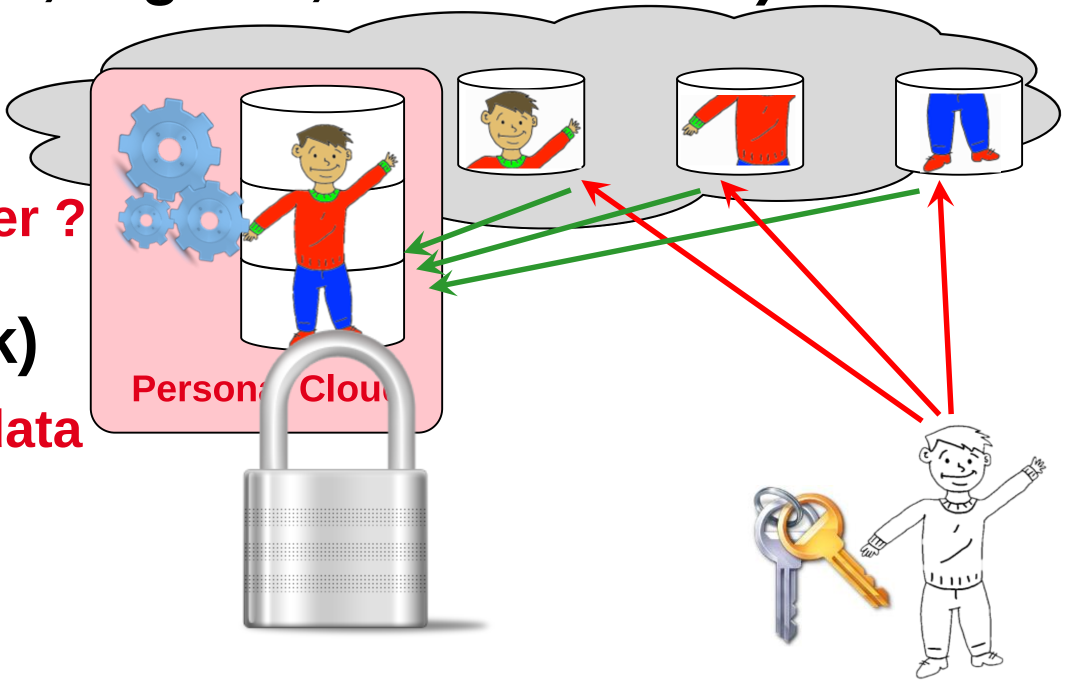
Wide variety of architectures, functionality, security

Online solutions (e.g., CozyCloud, Digi.me, BitsAbout.Me)

- The personal cloud provider
- … manages data and applications
- More responsibilities to the provider ?

Zero-knowledge (e.g., SpiderOak)

- The provider manages encrypted data
- … and the users manage the keys
- Shared responsibilities ?



Responsibilities induced by the technical choices ?

Wide variety of architectures, functionality, security

Online solutions (e.g., CozyCloud, Digi.me, BitsAbout.Me)

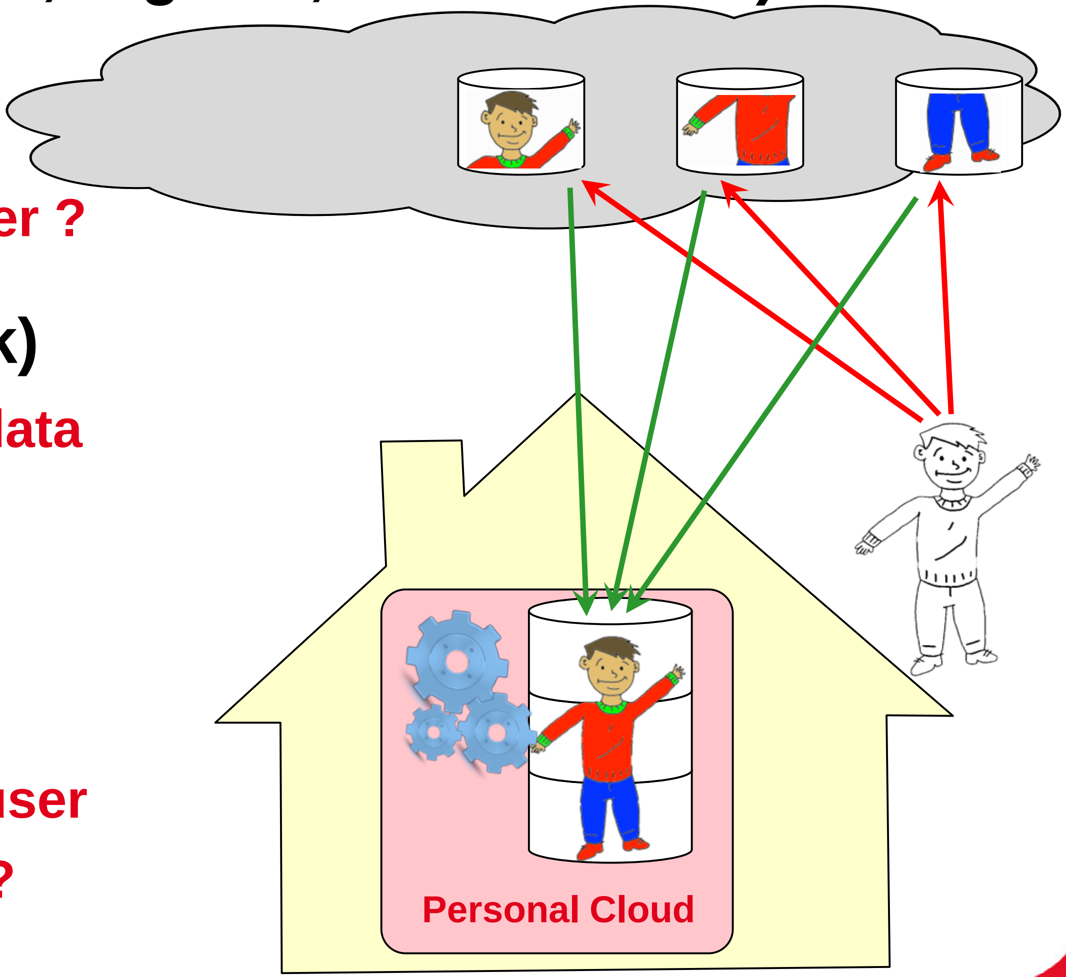
- The personal cloud provider
- … manages data and applications
- More responsibilities to the provider ?

Zero-knowledge (e.g., SpiderOak)

- The provider manages encrypted data
- … and the users manage the keys
- Shared responsibilities ?

Home cloud solutions

- Home server administered by the user
- More responsibilities to the users ?



GDPR, recent decisions, public policy objectives

GDPR context :

A new paradigm (accountability), new responsibilities (controller/processor)

A large scope of responsibility (CJEU, 5th June 2018, C-210/16)

Public policy objectives :

Balance between protection & innovation

Empowerment of individuals to promote their digital sovereignty

But a blind spot

How to take into account the proactive role of the data subject ?

Risk of “boomerang effect” ?

Cursor responsibility/sovereignty

Individualizing the protection tools of personal data and privacy

- **Taking into account the proactive role of the data subject**
- **Taking into account the reciprocal impacts between the technical architecture and the degree of “sovereignty”**

What about a graduate responsibility ?

- **Towards a cascading responsibility (stakeholder chain) :**
- **And a modular responsibility (case by case approach) ?**

Introducing secure hardware into the game

Powerful hardware, providing security guarantees, available everywhere

- ‘Trusted Execution Environments’ in PCs, smartphones/tablets & cloud
- AMD: Secure Execution Environment
- ARM: TrustZone
- Intel: Software Guard Extensions (SGX)

Example of Intel SGX ‘enclaves’

- Integrity/confidentiality of the computation (isolation from from the OS)
- Execution can be ‘stateless’ (leaves no trace)
- Integrity proof can be provided (attestation capability)
- Secure channel with the recipient of the computation (cloud)

What about secure hardware for the personal cloud ?

- Safe data collection, trusted computations …
- Audit guarantees to the actors based on their responsibility

Conclusion

GDP-ERE project's roadmap: from DATA to IA

- Investigate responsibilities along the data life-cycle
- Collection → storage → personal processing → crowd processing

Current step

- Graduate levels of responsibilities from collection to storage
- Investigate the impact of introducing secure hardware
- Assess legal & technical solutions to support the resulting liability

Next step

- Going from personal to crowd processing
- Support collective empowerment