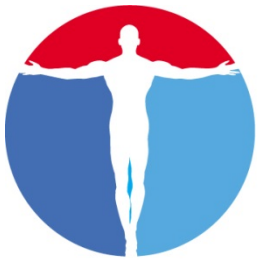


APDL

Association pour la Protection des Données au Luxembourg

GDPR- TECHNOLOGICAL IMPACTS

AGENDA

- General presentation
- Definitions
- Featured Articles
  - consent
  - simple, clear information
  - digital oblivion and erasing
  - data portability
  - profiling limitation
  - privacy by design / by default
  - record of processing activities
  - information in case of hacking
  - code of conduct and certifications
- Existing architectures: what are the challenges? How to prepare them?
- New regulation ⇔ new architectures
- 360° view
- Emergence of new services
- Conclusion

GENERAL PRESENTATION

- at the initiative of the **G29**
- repeals Directive **95/46 / EC**
- calendar:
  - **published** in the Official Journal of the EU on 4 **May 2016**
  - entered into force on **25 May 2016**
  - will have to be transposed into local law before 6 May 2018, for **effective application from 25 May 2018**
- applies to **any business located** in the EU or offering goods or services to **EU national**s (Article 3)
- principle of **accountability**: more prior declaration to the data protection authority (eg. CNPD), but an obligation to comply with the new regulation and to be able to demonstrate it (Article 22)
- appointment of a **Data Protection Officer** (DPO) for companies from a certain size (to be defined)

PERSONAL DATA?

Any data relating to an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

GDPR, Art. 4(1) (definitions)

Examples: lastname, firstname, bank details, birthdate/birth pace, fingerprints, number plate, email, social Security number…

PROCESSING?

Any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction.

GDPR, Art. 4(2) (definitions)

(UE) 2016/679 NEW REGULATION … FEATURED ARTICLES

- Articles 6, 7, 8: **explicit consent** required for one or more **specific purposes.** It must be as **simple** to withdraw consent as to give it
- Articles 12, 13, 14: right to be **informed** in a **simple and clear** manner
- Article 17: right to **digital oblivion** and **erasing**
- Article 20: **data portability** in a commonly used structured format **allowing re-use** of data by the data subject or a third party of his choice
- Article 21: clear **profiling limitation**
- Article 25: privacy **by design** / by default
- Article 30: establishment of a **register of treatment activities**
- Articles 33, 34: right to be **informed** in the event of **data piracy**
- Article 40, 42: progressive introduction of **code of conduct** and **certifications**

CONSENT

'The data subject's consent' means any freely given specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed. (GDPR, Art. 4)

- Legality of processing (Article 6): processing is lawful only if it meets at least one of these (main) criteria:
  - the data subject has **given consent**
  - necessary for the **performance of a contract**
  - necessary for compliance with a **legal obligation/regulatory**
  - necessary for the performance of a task carried out in the **public interest**

  ➔ treatment not falling within one of these criteria is prohibited
- Article 7: controller must be able to provide proof of consent ➔ it is necessary to keep, for each treatment, the information on the collection of the consent (nature, date …)
- Article 7: « It is as simple to withdraw consent as to give it. »
- Article 8: If the person concerned by the treatment is **under 16 years of age**, consent must be given by the holder of parental responsibility ➔ if the person concerned is under the age of 16, propose the validation of a treatment concerning him via a link sent in an email to one of the parents. In addition to the processing details, the email may contain a link (with no validity limit) to withdraw consent (Article 7).

SIMPLE, CLEAR INFORMATION

- Article 12: any communication about treatment should be done « in a **concise, transparent, intelligible and easily accessible form, using clear and plain language** » ➔ programmed end of the famous « I've read and accept the terms and conditions », biggest Internet lie ☺.
- Article 13: when data are **collected from the data subject**, the data subject shall be informed in particular of:
  - details about the **controller**
  - a possible transfer of this data **abroad**
  - the data **retention period**
- Article 14: when data are **not collected from the data subject**:
  - same obligations as those provided by Article 13
  - the need to indicate the **source of the data**

DIGITAL OBLIVION AND ERASING

Physical removal of data as soon as possible in the following cases:

- data are **no longer needed** as part of the processing for which they were originally required
- the person has **withdrawn the consent** to the treatment justifying the collection of such data (see Article 7)
- the person exercises his **right of objection** (see Article 21)
- data were the subject of **unlawful treatment**
- **compliance** with a legal obligation defined by the EU where the Member State to which the controller is subject

If applicable, the subcontractors of the person responsible for processing the data to be erased will have to execute the operation.

DATA PORTABILITY

- Article 20(1): « The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a **structured, commonly used and machine-readable format** and have the right to **transmit those data to another controller** without hindrance from the controller [...] »
- Preamble 68 : « Data controllers should be encouraged to **develop interoperable formats that enable data portability.** » ➔ format of the file (XML, JSON ...), structure and naming of fields: the legislator leaves the standards emerged from themselves
- Article 20(2) : « In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another » ➔ development of API for such exchanges

LIMITATION OF PROFILING

- Article 4(4) (définition): « 'profiling' means any form of automated processing of personal data consisting of the use of personal data **to evaluate certain personal aspects relating to a natural person**, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements; »
- Article 21 : « The data subject shall have **the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data** concerning him or her [...], including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims. » ➔ setting up an opt-out mechanism for each treatment

PRIVACY BY DESIGN

- Article 25(1): « [...] the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement **appropriate technical and organisational measures, such as pseudonymisation**, which are designed to implement data-protection principles, such as data minimisation » ➔ *privacy by design*
- consists in **proactively** ensuring the processing of personal data from the design of a system
- appeared in the 1990s in Canada, under the impulse of Ann Cavoukian
- this is not (yet) formalized as a standard or standard; for the moment it is simply a framework
- **pseudonymisation**: consists in **rendering impossible** or, failing that, the most complicated possible **the attribution of a data to a person** ➔ data hash, clear separation (eg use of separate tables) between data allowing direct identification (name, surname ...) and other personal data
- **minimisation**: this involves collecting **the minimum data necessary** for the processing for which they are intended; and **limit their retention period** ➔ *privacy by default*

RECORD OF PROCESSING ACTIVITIES

- as defined in Article 30 : « Each controller and, where applicable, the controller's representative, shall maintain a **record of processing activities** under its responsibility. »
- must be made available to the **supervisory authorities** if need be (principle of accountability)
- main information to be recorded:
  - the **name and contact details of the controller** and, where applicable, the joint controller, the controller's representative and the data protection officer
  - the **purposes** of the processing
  - a description of the **categories of data subjects and of the categories** of personal data
  - where applicable, **transfers of personal data to a third country** or an international organisation
  - a **general description** of the **technical** and **organisational security measures**
  - the envisaged time limits for erasure

INFORMATION IN CASE OF HACKING

- as defined on Article 33: «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. »
- information to communicate:
  - the **nature of the personal data breach** including [...] approximate number of data subjects concerned and the [...] approximate number of personal data records concerned
  - communicate the **name and contact details of the data protection officer** or other contact point where more information can be obtained
  - describe the likely **consequences** of the personal data breach
  - describe the **measures taken or proposed to be taken** by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects
- the **persons concerned** by the breach of data **must also be informed**, as soon as possible(Article 34)

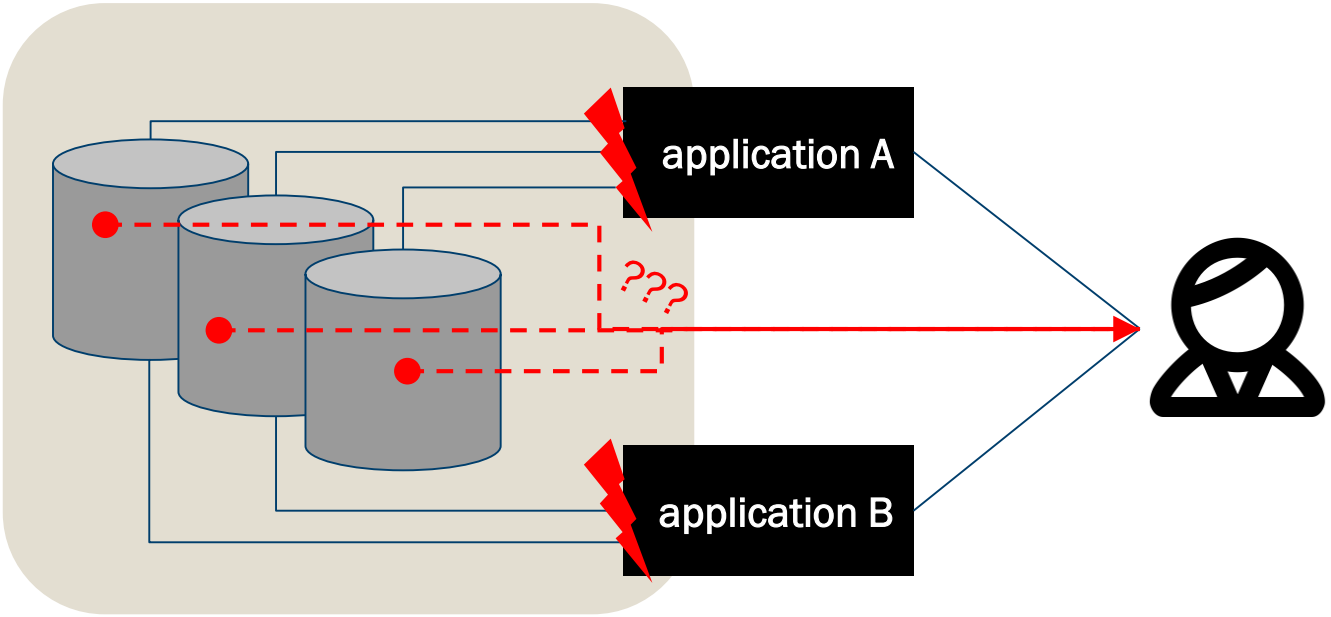
➔ implementation and/or reinforcement of measures to enhance security: encryption of databases at rest, encryption of all HTTP exchanges ...

CODES OF CONDUCT AND CERTIFICATIONS

- Article 40 encourages the **development of codes of conduct** designed to contribute to the proper application of Regulation
- « Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to: »
  - fair and transparent processing
  - the legitimate interests pursued by controllers in specific contexts
  - the collection of personal data
  - the pseudonymisation of personal data (➔ *privacy by design*, Article 25)
  - the information provided to the public and to data subjects
  - the exercise of the rights of data subjects
  - the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained (➔ Article 8)
  - the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects (➔ Articles 24 and 25).
- Article 42 provides for the establishment of certifications of conformity with Regulation

➔ the implementation of the principle of accountability will be guided by the appearance of these codes of conduct and the creation of these certifications

EXISTING ARCHITECTURES: WHAT ARE THE CHALLENGES ?

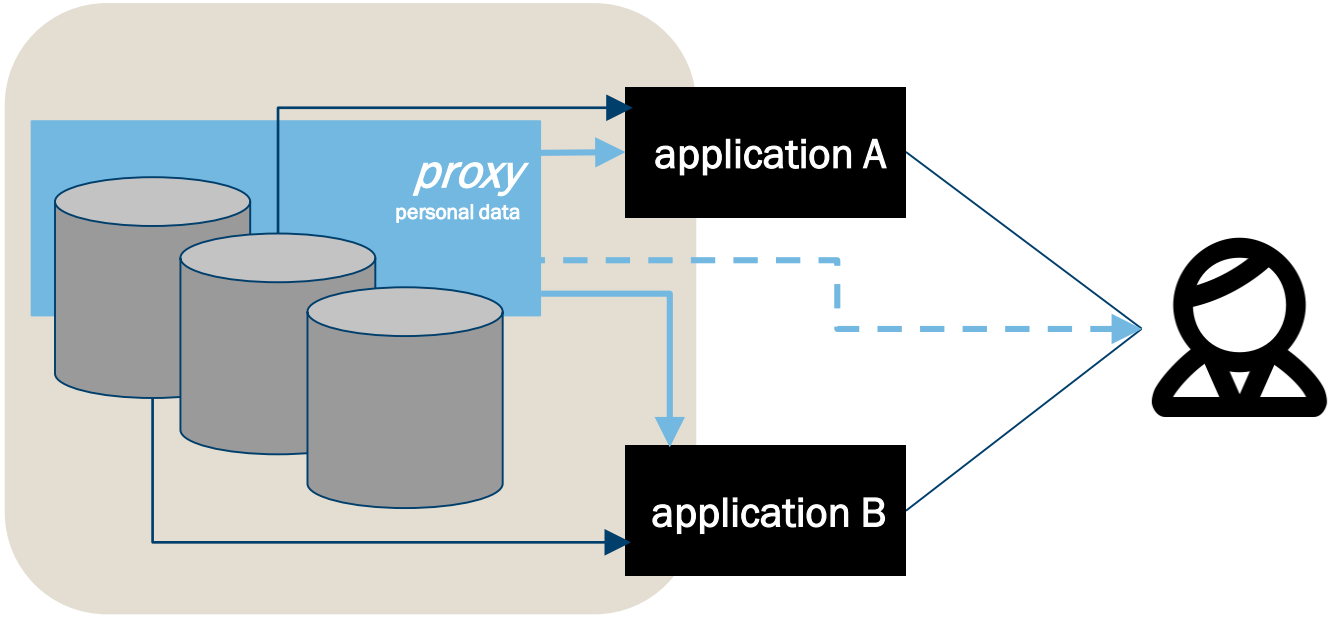


EXISTING ARCHITECTURES: HOW TO PREPARE THEM?

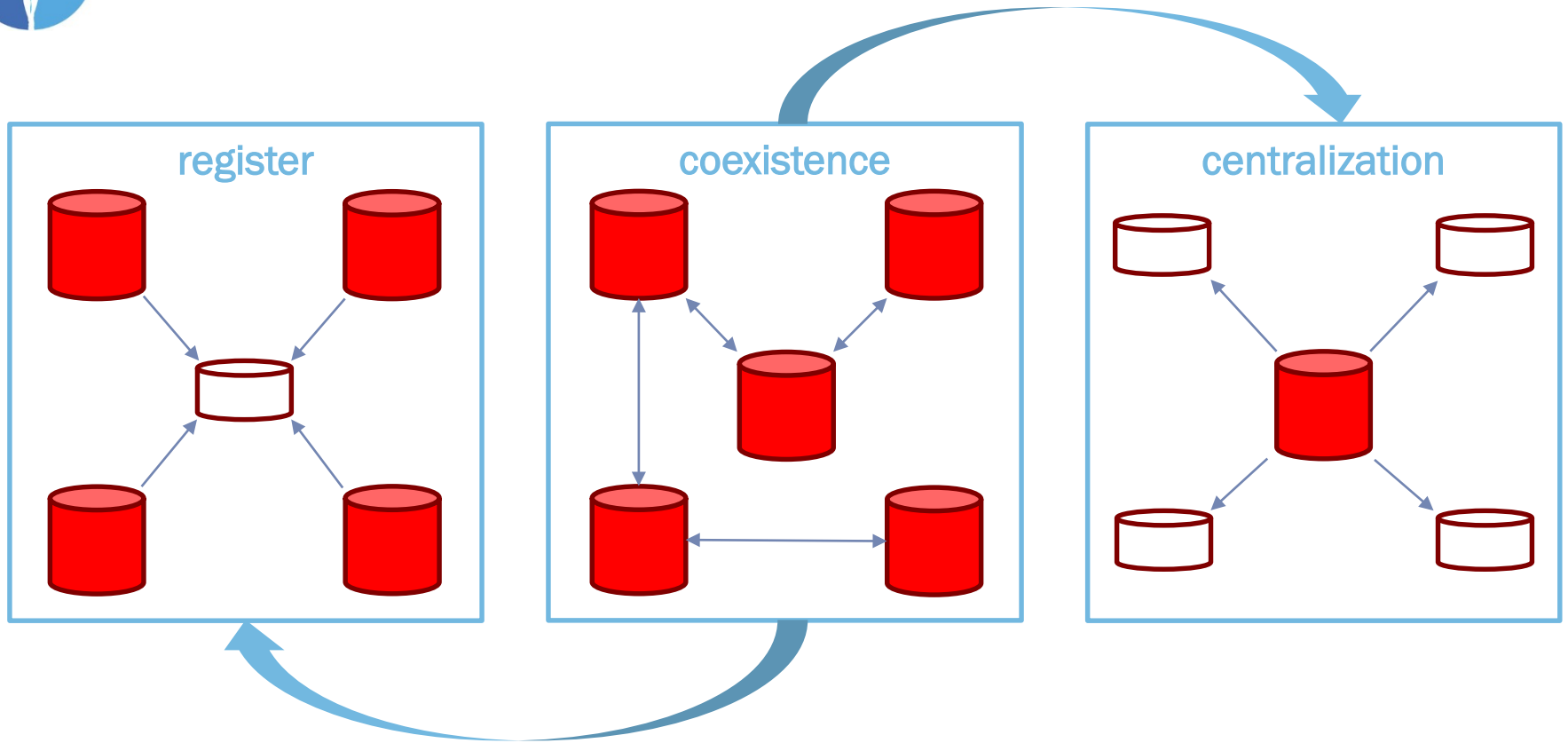
- **mapping**, covering the entire information system (including services provided by subcontractors, eg. cloud provider), the locations **where personal data are stored**
- for each of these data, add the following metadata:
  - **when** was it collected?
  - **reason** for the collection? treatment (s) applied to the data? (introduction of codifications)
  - **origin**: does the data come from the user himself or was it obtained from a third party?
  - applied **processings**?

➔ It is not too early to start this work! They should, whatever happens, be led to prepare for the GDPR

NEW REGULATION <=> NEW ARCHITECTURES...
SOLUTION PROPOSAL



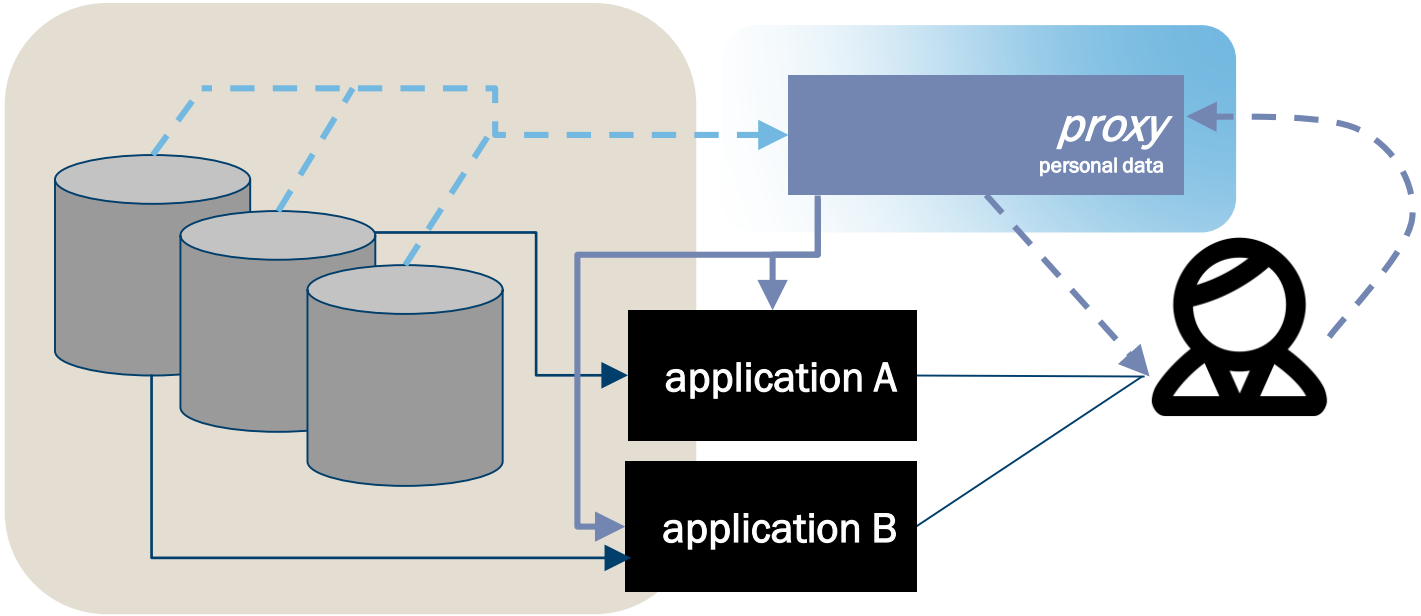
360° VIEW



360° VIEW – TWO STRATEGIES

- Register
  - **collecting the personal data in the different systems** and then consolidating them in a third-party system
  - provides a **single entry-point for searches** throughout the information system concerning personal data
  - relativly **simple to imple**ment; no or little impact on the existing information system
  - processes (initialization, update, deletion …) **continue to be done in the different systems**
- Centralization
  - creation of a **master record** for each client/user
  - could envolve **MDM platform** use; very expensive and complex to implement
  - **treatments are simplified**: they are made once at Masters level before being passed across the information system
  - potential blocking point: some of the systems **may not be designed to be updated** by an external process

EMERGENCE OF NEW SERVICES



CONCLUSION

- GDPR implementation concerns **almost all companies**
- **Important challenges** must be met in order to comply
- Necessity of **inventiveness to implement concepts** that are often not very formalized
- **Beware** of exceptions!
- Upcoming **certifications and guides**
- Great **opportunities to increase the quality** of information held