General Data Protection Regulation
(Banks & PFS)

Max SPIELMANN
Avocat
Schiltz & Schiltz

14 November 2016

uni.lu
UNIVERSITÉ DU LUXEMBOURG

APDL
Association pour la Protection des Données au Luxembourg

INTRODUCTION

- **GDPR** : Applicable as of 25 May 2018

- What will we look at?

  I. What is personal data?

  II. When to process personal data

  III. The principles of data quality

  IV. Accountability & your obligations

  V. Data subject rights

  VI. International data transfers

I. WHAT IS PERSONAL DATA

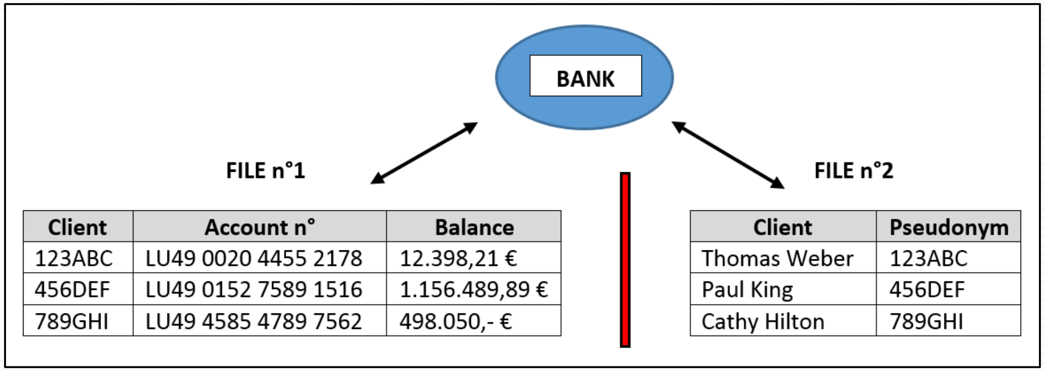
- **Definition**: "*Any information relating to an identified or identifiable natural person*"

- **"Anonymised" vs. "pseudonymised" data**
  - → Anonymisation = Person is no longer identifiable (No personal data)
  - → Pseudonymisation = Credentials are replaced by a pseudonym, but re-identification is possible (Personal data)

I. WHAT IS PERSONAL DATA - illustrations

- **Telephone banking**: Storing voice recods = <u>personal data</u>

- Keep client data in a **pseudonymised** format = <u>personal data</u>



Client	Account n°	Balance
123ABC	LU49 0020 4455 2178	12.398,21 €
456DEF	LU49 0152 7589 1516	1.156.489,89 €
789GHI	LU49 4585 4789 7562	498.050,- €

Client	Pseudonym
Thomas Weber	123ABC
Paul King	456DEF
Cathy Hilton	789GHI

- More difficult: **Anonymised** client data as to establish statistics (<u>ex.</u> Town of 12.000 inhabitants and 8 doctors):
  - Town, gender, age, occupation (no name or address) = <u>Personal data </u>("singling out")
  - Town, gender, age, "holds a university degree?" = <u>No personal data</u>

II. WHEN CAN I PROCESS PERSONAL DATA? - General

- **GDPR** = *A priori* identical to Dir. 95/46/EC

- **Legal bases** allowing for processing:
  - consent
  - contract (performance or entering into)
  - legal obligation
  - vital interests
  - public interest
  - legitimate interests (controller or third party)

Data processing

II. WHEN CAN I PROCESS PERSONAL DATA? - Consent

- **Consent** = *“any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”*

- **Conditions**:
  - proof that consent was given
  - intelligible and easily accessible form + clear and plain language
  - must be “freely given”

- **Right to withdraw consent at any time**

- **Consent under Dir. 95/46 remains valid** (if new conditions are met)

II. WHEN CAN I PROCESS PERSONAL DATA? – Legitimate interests

- **Allowed if:** Processing is necessary for the legitimate interests pursued

- **Limit:** Interests are overridden by those (including rights and freedoms) of the data subject

= Case-by-case approach

↓

Reasonable expectations of the data subject

- **Examples**:
  - necessary to prevent fraud
  - direct marketing purposes
  - network and information security
  - intra-group transmission of client or employee data

II. WHEN CAN I PROCESS PERSONAL DATA? – Further processing

- **Principle**: further processing must <u>not be incompatible</u>

➔ **But how to assess compatibility?**

- link between the initial and the new purpose
- context of the collection
- nature of the personal data
- possible consequences for the individual
- existence of appropriate safeguards

➔ Historical, statistical or scientific purpose = **always compatible**

- **Exception** (new):
  - consent
  - law

can serve to legitimise incompatible further processing

III. WHY SHOULD I CARE ABOUT DATA QUALITY?

- Data quality principles **apply to every data processing**

- **They include** (amongst others) the principles of:
  - purpose limitation
  - lawfulness, fairness and transparency
  - data minimisation

- The controller has to **demonstrate compliance** with these principles

  → *Accountability* principle

IV. ACCOUNTABILITY & OBLIGATIONS

- **Accountability** = Consequence of the *risk-based approach*

  → *Ex-ante* to an *ex-post* control

- **Accountability** = being <u>responsible</u> and demonstrate <u>compliance</u>

  - <u>Demonstrate compliance</u>… But how? (examples)

    → technical and organisational measures

    → keep records of those measures and your activities

  - <u>Being responsible</u> = risk of administrative fines for violations

    ➔ up to 20 million € or 4 % of the total worldwide annual turnover

IV. ACCOUNTABILITY & OBLIGATIONS

- **Your obligations** (as controller or processor) **are numerous**

➔ **You shall** (for example):

  - put into place technical and organisational measures
  - respect the principles of privacy by design and by default
  - designate, the case may be, a representative in the EU
  - only use processors providing sufficient guarantees
  - keep records of your processing activities
  - …

Obligations

- The GDPR also encourages the adoption Codes of conduct or the recourse to certifications

IV. ACCOUNTABILITY & OBLIGATIONS

Obligations

A. Choosing a processor (1)

- **For controllers:** Your processor must provide sufficient guarantees

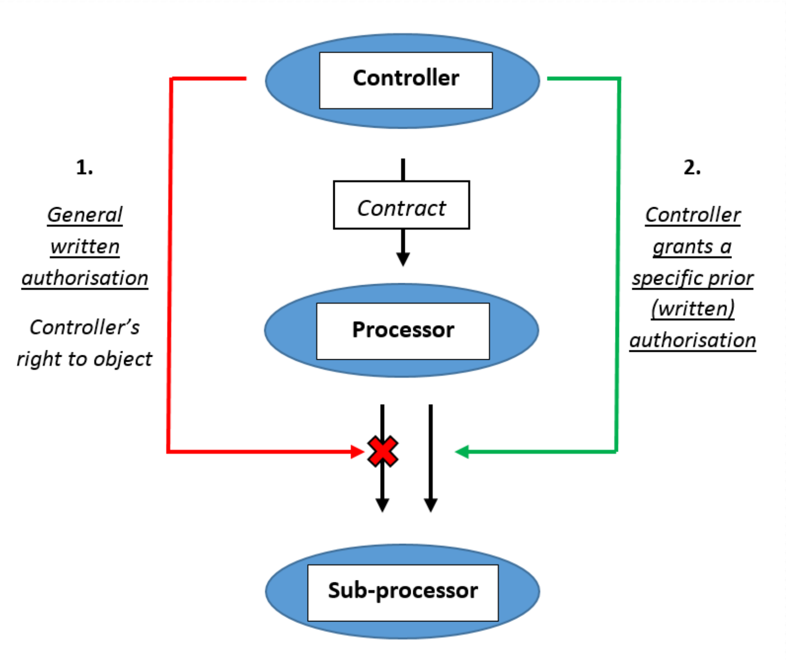
➔ Obligation to conclude a contract (or any other binding legal act) foreseeing the :

- subject matter and purpose pursued
- type of data concerned
- obligations to be respected by the processor
- …

IV. ACCOUNTABILITY & OBLIGATIONS

A. Choosing a processor (2)

- **Special case**: A processor has recourse to another processor


Controller
Contract
Processor
Sub-processor
1.
General written authorisation
Controller's right to object
2.
Controller grants a specific prior (written) authorisation

Obligations

→ Processor remains fully liable towards the controller

IV. ACCOUNTABILITY & OBLIGATIONS – B. Keep records

- **Principle:** Maintain records of processing activities

Obligations

- **Limit**: less than 250 employees + the processing entails no risk, is occasional and does not include special categories of data

For controllers	For processors
• contact details of the controller/DPO • description of the categories of personal data • categories of recipients to whom the data were (or are) disclosed • description of the international data transfers • description of the technical and organisational measures put into place	• contact details of the processor as well as of each controller for whom the data are processed • categories of processing activities • international data transfers • technical and organisational measures put into place

UNIVERSITÉ DU LUXEMBOURG

IV. ACCOUNTABILITY & OBLIGATIONS – C. Codes of conduct

- **Principle:** Associations or bodies representing controllers or processors may prepare Codes of conduct

  → Could be used to specify:

  - the legitimate interests pursued in specific situations
  - which security measures are appropriate
  - which data shall be collected
  - …

Obligations

- Codes of conduct have **3 main advantages**:
  - marketing
  - element to demonstrate compliance (sanctions)
  - international transfers

  → once approved (DPA + Commission) they may be used by an actor in a third country (condition = binding or enforceable commitments)

IV. ACCOUNTABILITY & OBLIGATIONS – D. Certifications

Obligations

- **General:** same advantages as Codes of conduct
- **Principles:**
  - DPAs set the conditions under which a certification may be issued
  - DPAs or accredited certification bodies (private actors) are then allowed to grant certifications
- Valid for a maximum period of **three years** (may be renewed)
- **Does not reduce the responsibility** of controllers or processors

V. DATA SUBJECT RIGHTS – Inform your costumers (1)

- **Distinction:** data are collected directly from the data subject <u>or</u> not (same structure as Dir. 95/46/EC)

- **More information** are to be provided under the GDPR (applies to both cases), for example on the:
  - → storage period
  - → legitimate interests pursued
  - → rights of your client
  - → right to lodge a complaint

- **Precision**: Data are not collected from the data subject

  → You have to give information as to the source of the data

V. DATA SUBJECT RIGHTS – Inform your costumers (2)

- **Limit:** the right to information is not absolute…

→ *But which exceptions do apply*?

Data are collected directly from the data subject	Data are not collected from the data subject
• Data subject already has the information	• Data subject already has the information • Providing information would involve disproportionate efforts • Providing information is "likely to render impossible or seriously impair the achievement of the objectives of that processing" • Data must remain confidential

V. DATA SUBJECT RIGHTS – Automated decision making (1)

- Every person = **Right <u>not</u> to be subject** to a decision which:

  (1) produces legal effects concerning him or her or similarly significantly affects him or her

  and

  (2) is based <u>solely</u> on automated processing, including profiling

- **<u>BUT</u>**: Right is <u>not</u> absolute → Exceptions

V. DATA SUBJECT RIGHTS – Automated decision making (2)

➔ **Allowed if** such decision:

- is authorised by law

  → law must foresee suitable safeguards

- is necessary for a contract (performance or entering into)
- is based on your client's explicit consent (new)

Here, the controller has to put the suitable safeguards into place

V. DATA SUBJECT RIGHTS – Automated decision making (3)

(Examples)

- **Bank offers online credit applications**
  - → legal basis for such decisions = ✓ (contract + consent)
  - → which suitable safeguards to put into place? (2 possibilities)

(1) Credit = granted	(2) Request = rejected
✓ (No further obligation)	Client shall have the right: • to express his or her view (human intervention) • be given an explanation of the decision • to challenge the decision

- **Online recruitment procedures** = Same guarantees apply

VI. INTERNATIONAL TRANSFERS - General

- **Principle:** International transfers of data are prohibited, unless the rules of the GDPR are complied with

- Possibilities = largely the same as under Dir. 95/46/EC
  - → adequacy decisions
  - → appropriate safeguards
  - → binding corporate rules (codified)
  - → derogations

VI. INTERNATIONAL TRANSFERS – *Non-repetitive* transfers (1)

*“**Where a transfer could not be based on** a provision in Article 45* [adequacy decisions] *or 46* [appropriate safeguards], *including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the **transfer is not repetitive**, concerns **only a limited number of data subjects**, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.”*

(Article 49(1) GDPR)

VI. INTERNATIONAL TRANSFERS – *Non-repetitive* transfers (2)

- ***No other legal basis exists*** = take it with a grain of salt

  → wording = result of a compromise solution (*trilogue*)

- "***Not repetitive***" (Council text = "not frequent" and "occasional")

  → shall not allow for <u>similar transfers</u> to be made on a <u>regular basis</u>

  → <u>residual character</u> = important

- "***Limited number of data subjects***" = No clarifications given

  → overall number of clients vs. costumers concerned (%)

  - nature of the data
  - purpose and duration of the processing
  - situation in the third country

CONCLUSION

The GDPR

(1) is complex and entails risks for controllers and processors

but

(2) offers new opportunities for those who know how to adapt

→ and that is why it is important to **be prepared** for 25 May 2018

Thank you - Merci - Danke

Max SPIELMANN
Avocat
Schiltz & Schiltz

uni.lu
UNIVERSITÉ DU
LUXEMBOURG

APDL
Association pour la Protection des Données au Luxembourg