The Rule of Law under Threat

Fall 2013
My children are my most precious asset

“The processing of personal data should be designed to serve mankind.

The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. “

General Data Protection Regulation (GDPR), Recital 4, par. 1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data
GDPR
What is new?

A bunch of stuff!

99 articles & 173 recitals

Fines of up to 4% of global turnover or 20 million €, which ever is higher... for starters

Figure 5: Crossreferencing of articles within GDPR (created by Sushant Agarwal, Institute for Management Information Systems, 2016)
GDPR structure

• Chapter I: General provisions
• Chapter II: Principles
• Chapter III: Right of the Data Subject
  • Section 1: Transparency and modalities
  • Section 2: Information and access to personal data
  • Section 3: Rectification and erasure
  • Section 4: Right to object and automated individual decision-making
  • Section 5: Restrictions
• Chapter IV: Controller and Processor
  • Section 1: General obligations
  • Section 2: Security of personal data
  • Section 3: Data protection impact assessment and prior consultation
  • Section 4: Data protection officer
  • Section 5: Codes of conduct and certifications
• Chapter V: Transfer of personal data to third countries or international organisations
GDPR structure (II)

• Chapter VI: Independent supervisory authorities
• Chapter VII: Cooperation and consistency
• Chapter VIII: Remedies, liability and penalties
• Chapter IX: Provisions relating to specific processing situations
• Chapter X: Delegated acts and implementing acts
Source: https://www.rizikon.oi/gdpr-compliance
Test 1: Does the GDPR apply to you?

It used to be, DPD art. 4:

Does the entity use any means of processing (automated or otherwise) located in any Member State?

It is under the GDPR (as of May 26 2018), art. 3:

Does the entity either
(i) Offer goods and services to EU residents; or
(ii) Monitor EU residents’ behavior?
Data types & the law

Some privacy law

Anonymous data

Possible privacy law?

Pseudonymous data

Privacy law

Personal data & PII

Sensitive data: health, financial, racial, political

Consent required!

Depends on variables and combinations

Hashing & encryption (by default)

Sensitive data:
- health
- financial
- racial
- political

Personal data & PII

Consent required!
The inevitable question! (≠ PII!)

Personal data in the GDPR (article 4.1)

‘personal data’:

any information relating to an identified or identifiable natural person (‘Data Subject’);

an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier

or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
I am a Data Subject
What I do for a living

In case you’re wondering ;-)
Interlocking liabilities & obligations

- Aligning contract obligations
  - (+ enforcement?)
- Providing
  - Security
  - Privacy features
  - Privacy engineering
Who? Data Controller – You? Data Processor

- **Data Controller**: You
- **Data Processor**: We, the data processor for this data flow, are also responsible for protecting it.
- **Privacy Rights**: Customers trust our clients to protect their data privacy rights in exchange for better products & services.
- **Preferred Tool**: Collect, use & protect people data for client.
- **Our Clients**: Collect, use & protect people data.

**Data Flow**

**Responsibility**

@aureliepols
An accountability chain
Once you know who you are

Art. 5: Principles relating to processing of Personal Data

“The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).”

Art. 6: Lawfulness of processing (a) to (f) options, typically consent or legitimate interest used
Consent, children, “sensitive data” & ePrivacy

Some privacy law

Anonymous data

Possible privacy law?

Pseudonymous data

Privacy law

Personal data & PII

Consent required!

Sensitive data: health, financial, racial, political, biometric, genetic

Depends on variables and combinations

Hashing & encryption (by default) enough???
And then consent means (article 4.11)

‘consent’ of the data subject means 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;

Note:

1. There can be multiple purposes and multiple consents given;
2. There is no structured information today about purposes... For some ideas, see [PayPal](#)
To make all that lawful (art.6)

2 things need to be specified:

1. **Purpose**: the reason for all this

2. **Consent**: the ok by the ‘data subject’

Note: **clients are responsible** for defining this (unless data is being passed along to another legal entity)
Macro vision of purpose & consent

Attributes of the database?
- Purpose
- Lawfulness of processing: one of the options of article 6.1 (a) to (f)

If (lawfulness of processing = legitimate interest), then
(consent field = description of legitimate interest)

If (records = personal data) & (lawfulness of processing = consent)
then Consent not null
Same idea at Apple (this is iOS 10)
MeNews uses cookies and other technologies, served by us and our partners, to... To learn more about each of our partners, see our Cookie Policy.

I consent to this data collection

Partners collecting data on this site:

Analytics Provider A  Opt-Out

Collects data about how you use this site, including your device configuration, where you are spending our time, and how you use our site.

Data Aggregator B  Opt-Out

Collects information about your use of this site and combines this information with how you use other sites to generate a profile of your interests for ad personalization across the web.

Ad Exchange C

Provides a marketplace that allows multiple marketers to assess ad inventory on...
Data Subject Rights

Chapter III
Data Subject Rights

• Art. 12: Right to Transparency
• Art. 13: What information should you provide? + Art. 14: same, if info doesn’t come from Data Subject
• Art. 15: Right of Access (not new!) => Subject Access Requests (SARs)
• Art. 16: Right to Rectification
• Art. 17: Right to Erasure (Right to be Forgotten, RTBF)
• Art. 18: Right to Restriction of Processing + Art. 19: Notification obligations
• Art. 20: Right to Data Portability
The coming of age of Transparency Wars?

Portability rights

http://tinyurl.com/PDIO-20170519
Right to Object & automated individual decision making
CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION

Article 1 on Human Dignity:
Human dignity is inviolable. It must be respected and protected.

Article 7 on Respect for private and family life
Everyone has the right to respect for his or her private and family life, home and communications.

Article 8 on Protection of Personal Data
1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority
GDPR: Re-introducing user’s rights into the data ecosystem

Fines: 4% of global turnover or 20 M €
Ok let’s talk obligations

Chapter IV
Controller & processor

• Art. 24: Obligations of the controller
• Art. 25: Data Protection by Design & by Default (pseudonymization & data minimization)
• Art. 26: Joint controllers
• Art. 27: Representatives not in the Union (for you aliens! => DPO)
• Art. 28: Processor
• Art. 29: Processing under the authority of the controller or processor
Want 1 GDPR goal? Aim for Article 30

Records of processing activities

The GDPR lays out a minimum of seven types of metadata that the inventories of data controllers must capture:

1. The name and contact details of the controller, the controller’s representative and the data protection officer;
2. The purposes of the processing;
3. A description of the categories of data subjects and the categories of personal data;
4. The categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international organizations;
5. Transfers of personal data to a third country or an international organization, including the appropriate safeguards relied upon to allow those transfers;
6. The envisaged time limits for erasure of the different categories of data; and
7. A general description of the technical and organizational security measures applied to that data.

Third-party vendors acting on behalf of data controllers—which are referred to as data processors—must maintain a similar but streamlined record addressing names and contact information, categories of processing, the transfers of personal data including safeguards, and the technical and organizational measures applied to that data.
What else do you need?

• Art. 32: Security of processing
• Art. 33: Notification of a personal data breach to the SA + art. 34
• Art. 35: Data Protection Impact Assessment (DPIA)
2 options to manage risk (putting aside data minimization*)

Security of Processing (art. 32)
- Pseudonymization & encryption, secure transfers, two level authentications, etc.
- The “CIA triad”: confidentiality, integrity, availability
- Resilience and restoration
- Regular assessment of security measures
- Certifications, codes of conduct (ranges from ISO 27k to Cobit to OWASP...)
- Alignment of purposes

De-identification (the US likes that, similar to pseudonymization yet no Privacy obligations!)

* Data minimization is a basic Privacy principle yet still a difficult reflex in large scale digital set-ups
@aureliepols
Identification capabilities is a **TRUST** issue

From Understanding Privacy principles and ensuring confidence of your digital activities by Aurélie Pols, AT Internet, May 2016
International data transfers?

Data localization initiatives around the world
The curious case of the (evolution of the) US

• Federal laws, state laws, sectorial laws (HIPAA, COPPA, VPPA, Fair Housing Act)

• Supervisory Authority:
  • FTC, FCC??: Section 5, ISPs
  • local Attorney Generals?

• Wyndham case for security

Preparing for May 2018

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)
## Initial GDPR Pillars: what you need to prepare for

### i. Data Security & Breach notification

**Owner:** TBD

- What exists today?
- Ongoing continuous documentation exist?
- Consolidation of Breach notification processes?

### ii. Codes of Conduct & Certifications

**Owner:** TBD

- Are they required (by partners for eg.)?
- If so, which ones?
  - security / data protection
  - privacy
- Are they defined?
  - Ethical data uses for insurance sector for eg.?

### iii. Classification of data types (Pseudonymous, personal data, ...)

**Owner:** AP + Legal Support: TBD

- Probably the bulk of the work after iv. Use case classification
- Will require:
  - keeping internal definitions 4 balance with legal + security measures
  - mapping: listing, flows and deletion

### iv. Data subject consent

**Owner:** AP + Legal Support: TBD

- Requires definition of use cases through contract analysis first.
  - Followed by functionalities & processes required to support consent mechanisms (cf. vii.), certainly for (LT?) data market place, in light of iii. & v. + documentation!

### v. Profiling & the Right to Object

**Owner:** TBD

- Definition of profiling, applicable to you?
- To be analyzed:
  - does profiling apply?
  - What would the right to object require?

---

@aureliepols

Confidential – prepared by Aurélie Pols
GDPR: on top of what should also be considered

vi. Cross border data transfers
Owner: procurement?

Where does the data sit (SaaS/cloud), under which jurisdiction & is this acceptable to clients / customers?

List tools used, map to iii., review Terms & Conditions

vii. The New Rights to be Forgotten / Deletion
Owner: TBD

Owner: TBD

viii. (Data Portability)

Perviously applicable, maybe not yet today. Should be monitored for best practices + evaluated in terms of practicability & documented

ix. Duties & responsibilities, data processor

Owner: Legal/compliance

Support: GDPR program members

Documentation responsibility
Redistribution of 5+5 pillars, defining ownership

x. Procedures & Fines

Owner: Legal/Compliance

Possibly applicable, maybe not yet today. Should be monitored for best practices + evaluated in terms of practicability & documented

Should be monitored for best practices + evaluated in terms of practicability & documented

Standard operating procedures (SOPs) + keeping communication line open with
- (Belgian?) DPA,
- HQ?
- Industry bodies?
- ...

confidential – prepared by Aurélie Pols
Data Governance & Privacy Engineer

Data is the New Oil – Privacy is the New Green – Trust is the New Currency
Dutch nationality, French mother tongue, works in English, lives in Spain

- Chief Visionary Officer – Mind Your Privacy
- Ethics Advisory Group – European Data Protection Supervisor (EDPS)
- Training Advisory Board – International Association of Privacy Professionals (IAPP)
- Professor of Data Governance, Privacy & Ethics – IE (Spain), Solvay Business School (Free University of Brussels), Maastricht University
- Co-chair P7002 – Data Privacy Process - IEEE

@aureliepols
Thank you so much for your time

@aureliepols