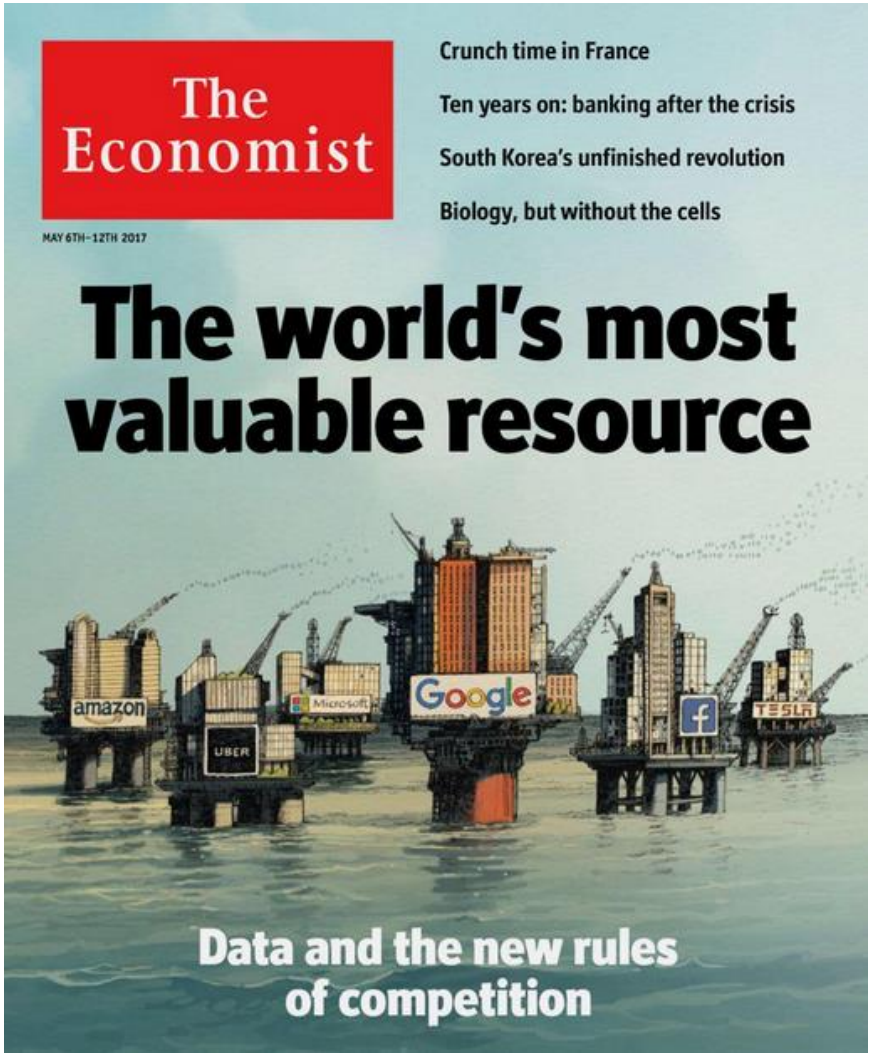
EU GDPR - General Data Protection Regulation

mag. Andrej Tomšič

Deputy Information Commissioner

Living bits and things

Bled, 19 June 2017


The Economist
MAY 6TH–12TH 2017
Crunch time in France
Ten years on: banking after the crisis
South Korea's unfinished revolution
Biology, but without the cells
The world's most valuable resource
amazon
UBER
Microsoft
Google
TESLA
Data and the new rules of competition

By Source, Fair use,
https://en.wikipedia.org/w/index.php?curid=13627120

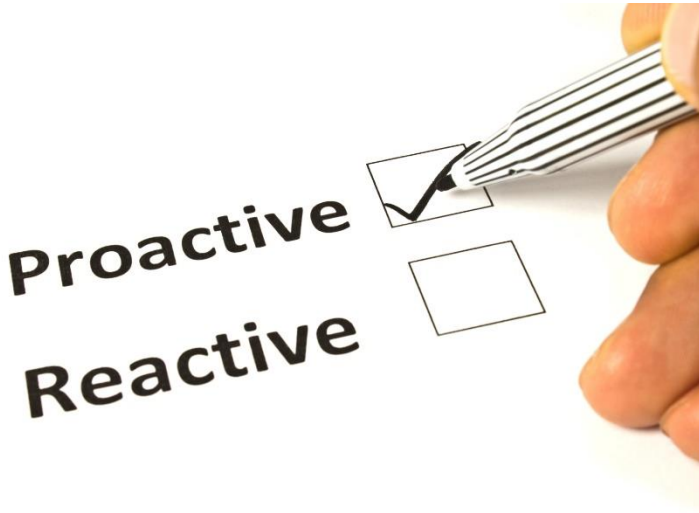
REGULATION (EU) 2016/679

General Data Protection Regulation (GDPR)

Principles relating to processing of personal data

Article 5

- lawfulness, fairness and transparency
- purpose limitation
- data minimisation
- accuracy
- storage limitation
- integrity and confidentiality
- **accountability**
  - The controller shall be **responsible for**, and **be able to demonstrate compliance** with basic principles.
  - More emphasis on **proactive** and **preventive** measures.



Data portability

Article 20 - Right to data portability

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,where:

a) the processing is based on consent or contract,
b) the processing is carried out by automated means.

- Not applicable for paper files, processing in public interest.
- Shall not adversely affect the rights and freedoms of others, e.g.:
  - Intelectual property rights
  - Rights of other data subjects.

Data protection by design and by default

Article 25

- Taking into account the **nature**, **scope**, **context** and **purposes** of **processing** as well as the **risks** of varying **likelihood** and **severity** for the rights and freedoms of natural persons

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** and to integrate the **necessary safeguards**.

by default, only personal data which are necessary for each specific purpose of the processing are processed**:**

- **the amount of personal data collected,**
- **the extent of their processing,**
- **the period of their storage and**
- **their accessibility**.

- Certificate may demonstrate compliance.

Processors and records

Article 28 – Processors

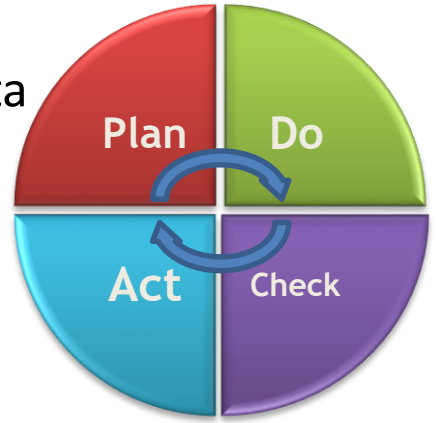
- Only processors providing **sufficient guarantees shall be used.**
- Processor shall **not engage another processor without prior specific** or **general written authorisation** of the **controller**
  - Hosting, cloud and other IT providers!
- **More requirements for contracts with processors:**
  - the **subject-matter** and **duration** of the processing,
  - the **nature** and **purpose** of the processing,
  - the **type of personal data** and
  - **categories** of data subjects and
  - the **obligations** and **rights** of the controller,
  - only **under instructions** of data controller…

- **Article 30 - Records**
  - **Apply also to processors!**
  - **No more notifications** to central registers.
  - Questionable exemptions for SMEs…

Security of processing

Articles 32, 33, 34

- **Technologically neutral principles**
  - pseudonymisation and encryption of personal data
  - Process for **regularly testing, assessing and evaluating** the effectiveness of technical and organisational measures
  - **codes of conduct** and **certificates**



- **Mandatory breach notification to supervisory authority**
  - Within 72 hours
  - Processor to inform data controller
  - Impact on administrative fines

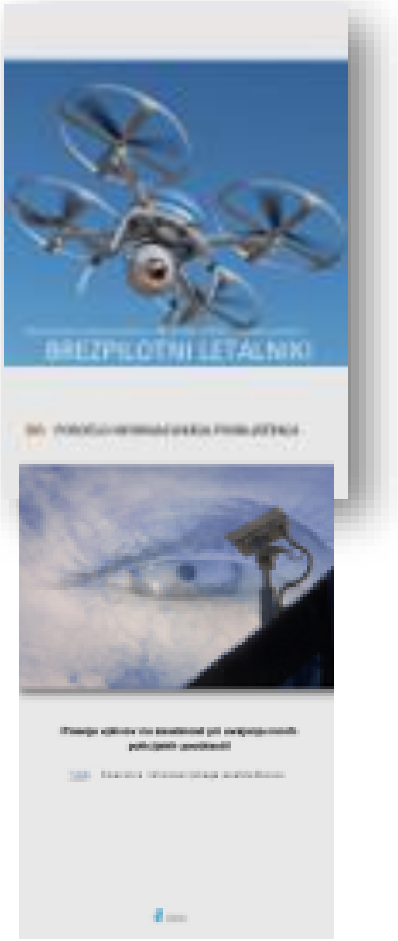
- **Notification to data subjects**
  - In extreme cases
  - Not necessary under certain condition (e.g. adequately encrypted data)
  - Public notification also possible

Data protection impact assesments

Article 35

- Where **high risks** - data protection impact assesment
  - DPA/EDPB guidelines
  - E.g. new IoT application, smart-city projects, e-ticketing, location tracking, profiling…
- **Data Protection Officer** should be consulted.
- **DPIA required in particular**:
  a) **automated decision making**, including **profiling**;
  b) processing on a large scale of *special categories* of personal data or personal data relating to criminal convictions and offences; or
  c) systematic monitoring of a publicly accessible area on a large scale.
- DPAs/EDPB to **determine a list of processing operations** which are (not) subject to data protection impact assessment.

Drones, police powers:



Data protection officers

Articles 37, 38, 39

<u>Controller and processor to nominate a DPO:</u>

- Public bodies except courts
- Systematic processing of personal data/profiling
- Processing on a large scale of special categories of personal data

DPO:

- on the basis of **professional qualities** and **expert knowledge** of data protection **law and practices**
- may be a **staff member** or external („**DPO-as-a-service**“)
- publish the **contact details** of the DPO and communicate them to the supervisory authority
- **monitoring and advisory role**
- may fulfil **other tasks and duties** (*conflict of interests)
- does not receive any **instructions**
- **supported** by controller/processor
- responsiblity, fines?

Codes of conduct and certification

Article 40-43

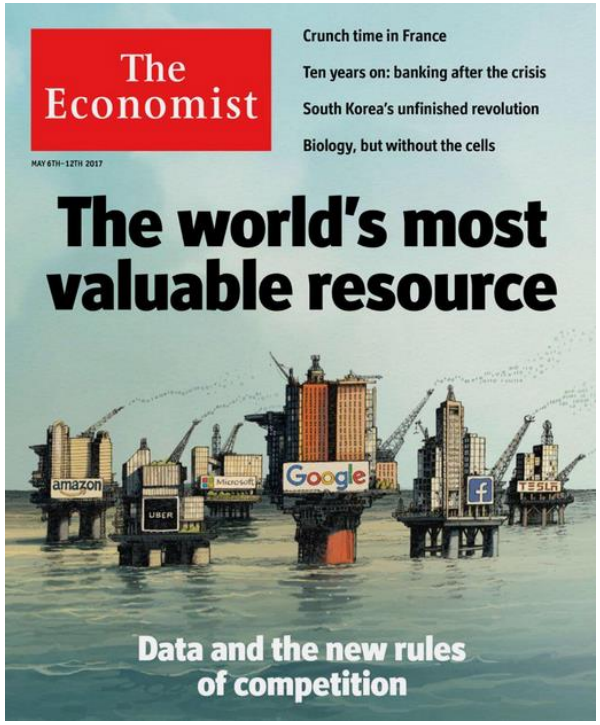
Codes of conduct

- Interesting for **associations** and other **bodies representing categories of controllers or processors**
- May cover different **topics** (e.g. standard contracts with processors, breach notification, collection of personal data…)
- **Approved** by DPA/EDPB
- Could **assist SMEs/start-ups** in compliance requirements

Certification

- data protection certificates, **seals** and **marks** -
- **scope: processing operations**
- **voluntary**
- By **supervisory body** or **accredited certification bodies**
- Valid for 3 years, can be revoked/extended
- Does not reduce the responsibility
- Impact on fines?

Maybe we will slowly begin to understand the *true value* of our data…



Thank you for your attention!

andrej.tomsic@ip-rs.si
@tomsandrej