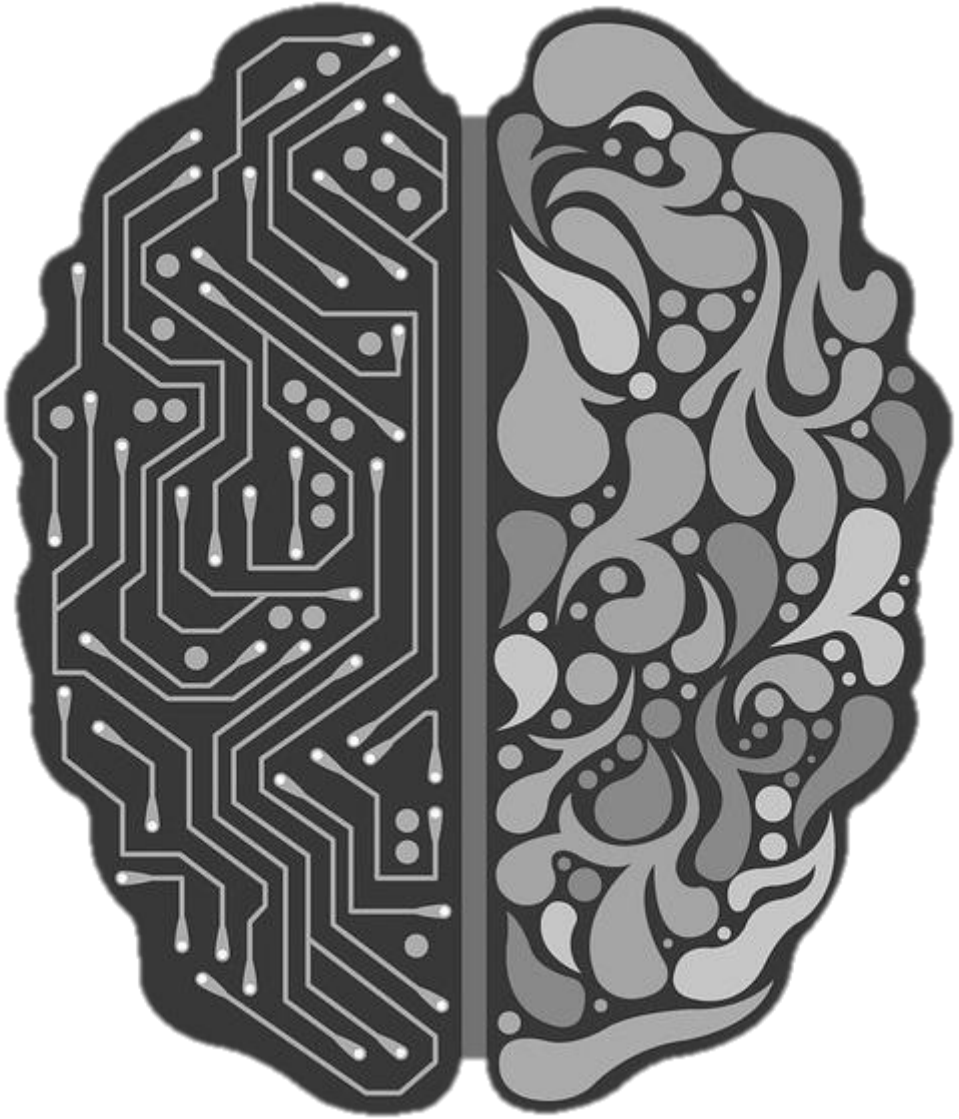
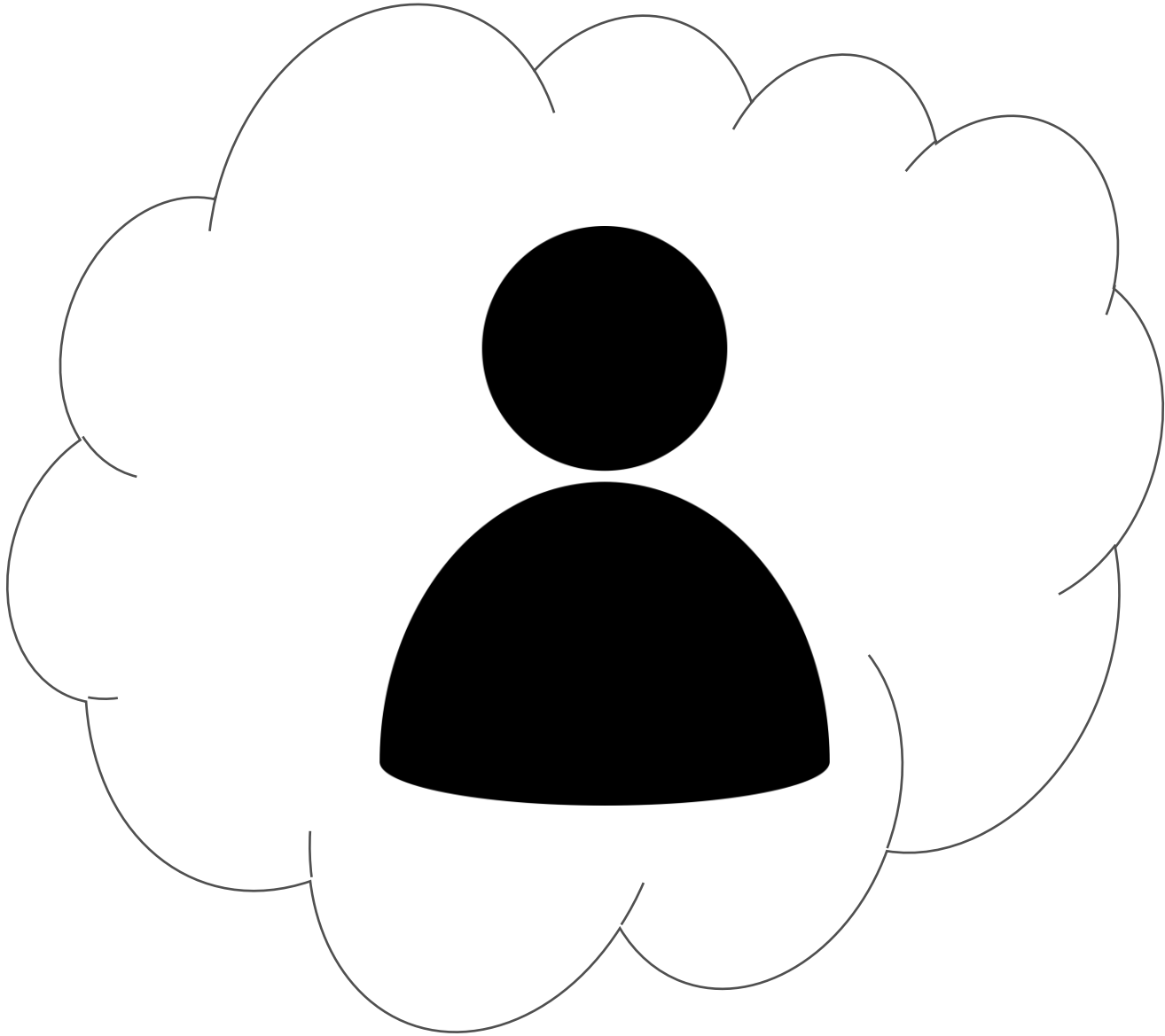
COBALT

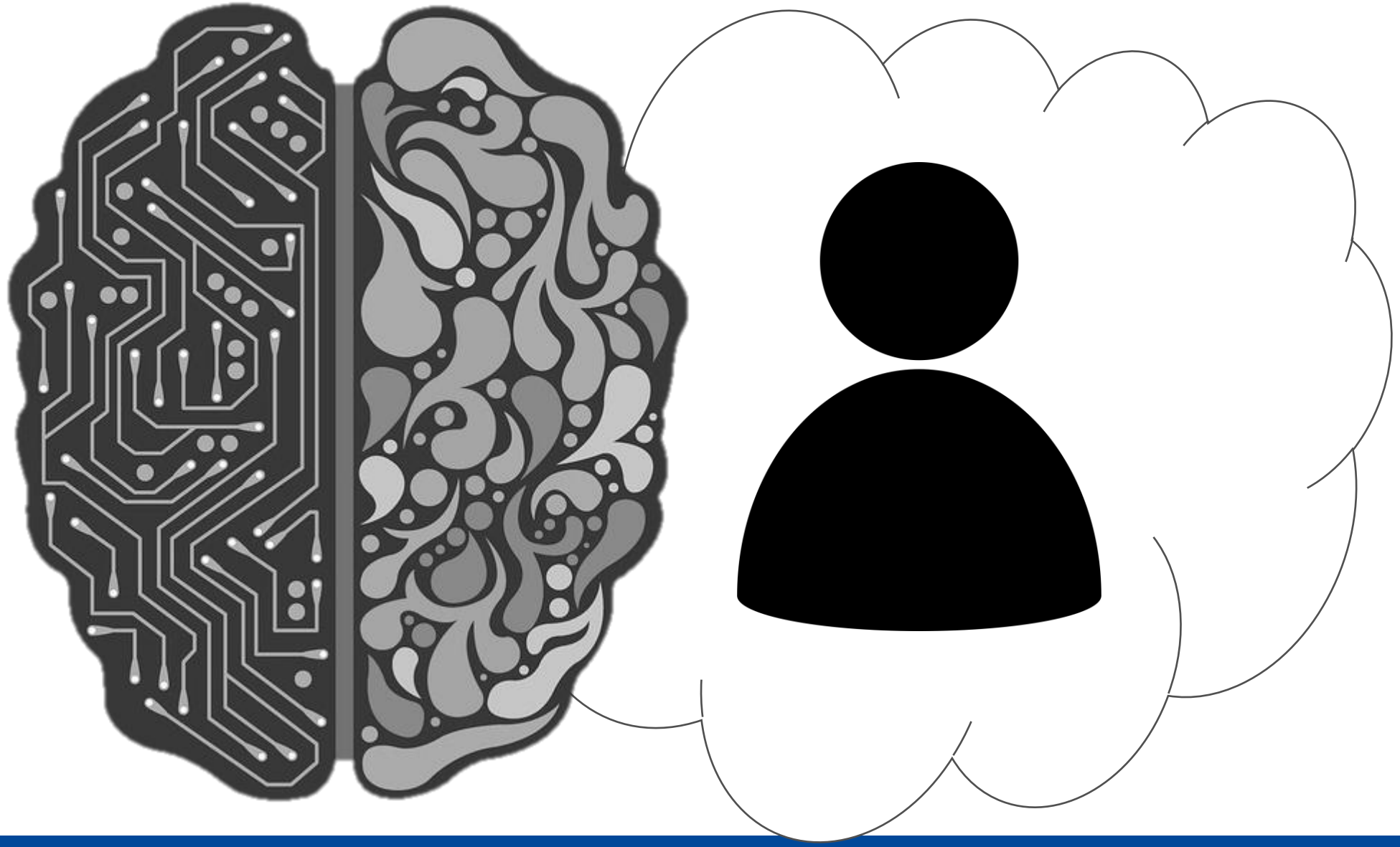
IS IT POSSIBLE TO PROGRAM DATA PROTECTION AND PRIVACY IN (IF WE DO NOT KNOW WHAT IT MEANS)?

Anna Vladimirova-Kryukova, CIPP/E, Certified DPO

17 October 2019

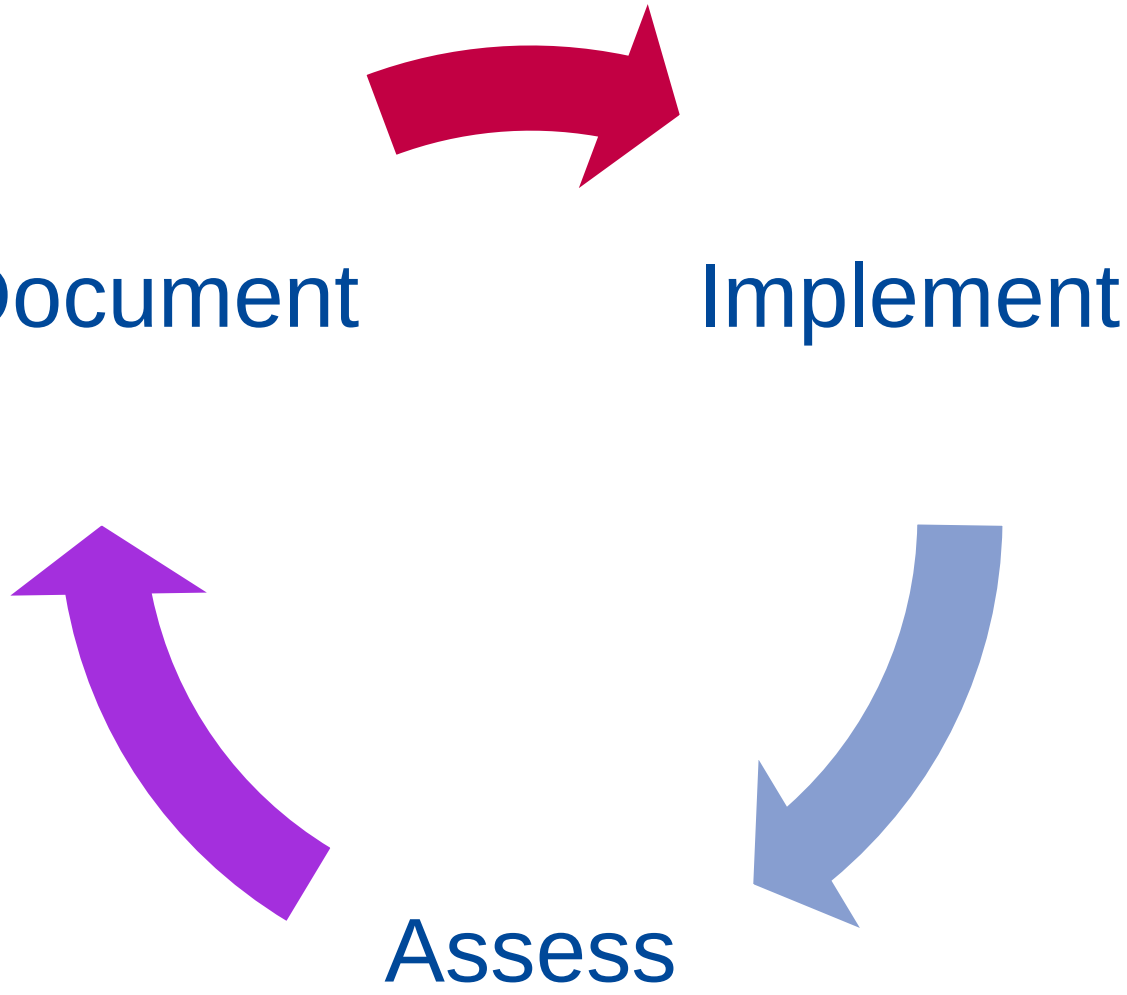






Privacy by design **vs** **Data protection** by design and by default (+ personal data security)

WIDE INTERPRETATION?


Document
Implement
Assess

GDPR

Integrity and confidentiality principle:

- appropriate **security**
- protection against **unauthorised or unlawful** processing and against **accidental loss, destruction or damage**
- appropriate **technical or organisational** measures

GDPR

Data protection by design:

- appropriate **technical** and **organisational** measures (e.g. pseudonymization)
- **designed** to implement data-protection **principles**
- in an **effective** manner
- **integrate** the necessary safeguards into the processing
- meet the **requirements of the GDPR** and protect the **rights of data subjects**

GDPR

Data protection by default:

- **technical** and **organisational** measures
- **by default**
- only personal data **which are necessary** for **each specific purpose** of the processing are processed
- applies to the **amount** of personal data collected, the **extent** of their processing, the **period** of their storage and their **accessibility**
- personal data **are not made accessible** without the individual's intervention **to an indefinite number of natural persons**

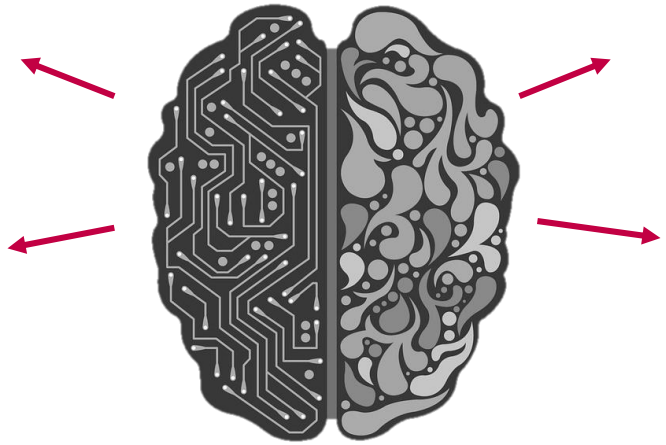
GDPR

Personal data security:

- **technical** and **organisational** measures
- ensure a level of security **appropriate to the risk**

GDPR

- **Technical solutions**
  - Pseudonymisation and encryption
  - Confidentiality, integrity, availability and access
  - Resilience
  - Testing, assessing and evaluating
  - Measures from specific cases
  - Standards and guidelines (ISO, NIST, ENISA)



- **Organizational solutions**
  - Risk analyses
  - Policies
  - Business mechanisms
  - Trainings
  - Third parties
  - DPIA

GDPR

GDPR

ACTION
(insider and third party)

INCOMPLIANCE

GDPR

Transparency:

Information on the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) of the GDPR and, at least in those cases, **meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject**.

GDPR FINES

50t

645t

30t

460t

230M

230t

15t

130t

2,6M

110M

62t

180t

EXAMPLES

- No updates for software, not applying updates to al systems and devices used
- Using unsupported OS
- Poor practices in maintaining source codes
- Skipping a testing phase / vulnerability scanning / pentesting / audits
- Running unnecessary services
- No maintaining for legacy systems
- Poor password policies and password storage, default credentials
- Absence of encryption for communication channels
- Problems with managing certificates
- Problems with backups

EXAMPLES

- Logging issues and their secure storage
- Managing access rights
- Problems with building teams
- Sharing accounts
- Absence of data mapping
- Poor identity protection
- Disproportional tracking techniques
- Giving users too much freedom vs. pre-checking something instead of users (ENISA: minimize, hide, separate, aggregate, inform, control, enforce, demonstrate)
- Poor maintenance practices

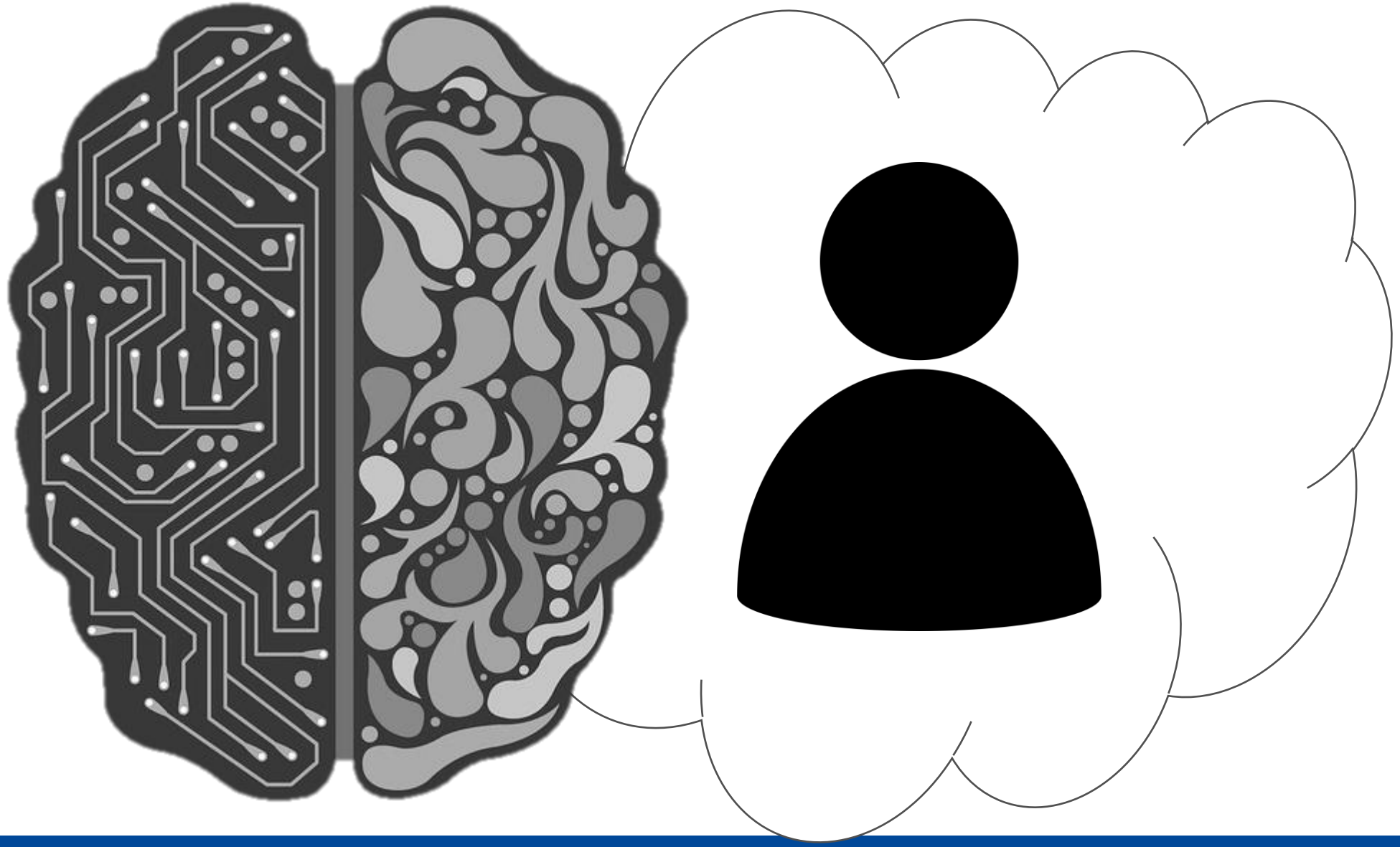
EXAMPLES

- Données & Design – CNIL initiative (France)
- Cyber Essentials – National Cyber Security Center (UK)
- Guidelines relating to IT-security and managing cyber security threats - the Danish Centre for Cyber Security and the Danish Agency for Digitisation.
- Description of security levels (1 to 4) and the minimum requirements for each security level - Lithuanian Data Protection Authority.

WIDE INTERPRETATION

“ The interface is the first object of mediation between the law, rights and individuals.”

CNIL



DATA NEWS

https://www.subscribepage.com/g2s0o2

Thank you!

Estonia
Kawe Plaza, Pärnu mnt 15
10141 Tallinn
Tel +372 665 1888
tallinn@cobalt.legal

Latvia
Marijas iela 13 k-2
LV-1050 Riga
Tel +371 6720 1800
riga@cobalt.legal

Lithuania
Lvovo 25
LT-09320 Vilnius
Tel +370 5250 0800
vilnius@cobalt.legal

Belarus
Pobediteley Ave 100-207
220020 Minsk
Tel +375 17 336 0093
minsk@cobalt.legal

www.cobalt.legal